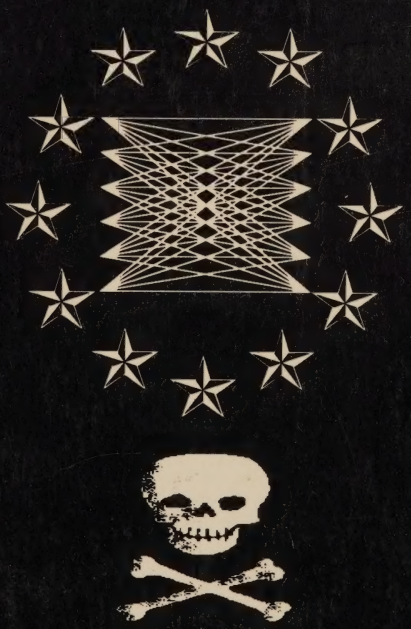
European Scrambling Systems

John McCormac

4



The Black Book

European Scrambling Systems

Circuits, Tactics And Techniques.

4

The Black Book

John McCormac

Waterford University Press

An imprint of MC2 (Publications Division)

European Scrambling Systems

Circuits, Tactics And Techniques.

4

John McCormac

Legis Cautio Contra Ineptos Criticos

Qui legent hos versus, mature censunto;
Prophanum vulgus et inscium ne atrectato.
Omnesque Astrologi, Blenni, Barbari procul sunto,
Qui aliter faxit, is rite sacer esto.

Waterford University Press

An imprint of MC2 (Publications Division)

All Rights Reserved.

Copyright (c) 1988, 1989, 1990, 1991, 1992, 1993, 1994

John McCormac.

This edition is published by:

Waterford University Press

MC² (Publications Division)

22 Viewmount, Waterford, Ireland, EC

Telephone: + 353-51-73640 (After 1400 Hrs GMT)

Fax: + 353-51-73640

BBS: + 353-51-50143 HST 14K4 8N1 ANSI

All rights reserved. This book is sold subject to the condition that it shall not, by way of trade or otherwise, be lent, re-sold, hired out, or otherwise circulated without the author's prior consent in any form of binding or cover other than that in which it is published and without a similar condition including this condition being imposed on the subsequent purchaser.

No part of this publication may be reproduced or transmitted without the written permission of the copyright holder.

The information herein is for educational use. The publishers and the author do not accept any liability for its use or misuse by the reader.

All trademarks are acknowledged.

ISBN Number: 1-873556-03-9

Printed in Ireland by: MC2 (Publications Division)

Acknowledgement

To my parents and family - thanks.

I would like to thank all who helped in the compilation of this version who for reasons of security must remain anonymous.

European Scrambling Systems

Circuits, Tactics And Techniques

4

Table Of Contents

Chapter 1... The Story So Far

Chapter 2... The Principles Of Security

Chapter 3... Descrambler Building Blocks

Chapter 4... Audio Scrambling Techniques

Chapter 5... Dirty Tricks

Chapter 6... Cracking The Code

Chapter 7... Video Manipulative Scrambling Systems

Chapter 8... Cable And Microwave Distribution

Chapter 9... Descrambler Hook-Ups

Digitized by the Internet Archive
in 2024 with funding from
Amateur Radio Digital Communications, Grant 151

https://archive.org/details/europeanscrambli04mcco

An Introduction To Scrambling

The first law of magic is that chaos is order and order is chaos. This is a proven mathematical fact. It is also the first law of hacking. In order for the scrambled signal to be recovered, there has to be some sort of order in the scrambled signal. The more secure systems use digital techniques but despite their complexity, they are not ultimately secure.

The fun or thrill of hacking is breaking a system that cost millions to develop with a few pence worth of components. It is a common fallacy that if the subscription cost of a system was reasonable hackers would not attempt to hack that system. This argument is generally proposed by JAFAs. for those still wondering what JAFA means, it is an acronym for Just Another F*%&ing Amateur.

Hacking is a game of technological chess and as with any sport nowadays there are amateurs and professionals. Luckily for the hackers the greater proportion of the system users are non-technical business people and hence by the above definition, amateurs.

The information in the book should be equally valuable to system owners and to hackers. The system owner has the most to lose and the hacker has the most to gain. It will give the system owner access to information about hacking that he or she would not otherwise be able to obtain. It should also give the reader, regardless of side, a detailed knowledge of the practice of signal security.

Those words were written in 1988. Since that time, the satellite and cable television markets have mushroomed. So has the Blackbox business. Despite all of the protestations of the advertising and publicity people, the business of piracy has survived. In fact it has become an industry that was worth an estimated three hundred million

pounds in Europe in the last year. That is approximately half a billion dollars. Ironically this was more than many of the pay television channels earned in the same time period.

Pick up some European satellite television magazines and you are likely to run across adverts for pirate smart cards or decoders before you get to any articles. Even in America, land of the brave and home of the fee, magazines carry adverts for the monthly codes for VideoCipher. With the US legal system, you've got to be brave to be in the US Blackbox industry.

In Europe there is no coherent Europe-wide legal framework for dealing with piracy. It is generally a case of each country protecting its own channels or channels that uplink from their country.

This situation is not working very well. In the UK it would seem that the average person who goes for a third party Sky card regards it more as an act of resistance against the empire of Murdoch. Rupert Murdoch is of Australian origin so there may be some curious patriotic influence at work as well.

The air of illegality adds to the risk. The third party smart card is like the ultimate faceless crime. It is difficult to track down as the dealers rarely keep records of the customer's names and addresses.

Perhaps the reason that the Blackbox Industry thrives is stupidity. The stupidity lies mainly in the policies of the management of the channels under attack.

Of course it is a sweeping generalisation to say that all channels are similarly afflicted. Some channels take the matter of piracy seriously and have plans to deal with the eventualities. Perhaps "eventualities" is the wrong word. It doesn't convey the uncertainty of imminent doom.

It is very difficult to envisage a totally secure system. For a start, the military interest groups would not permit the open use of such a system. After all they need to be able to access everything that is transmitted. The other factor is that the amount of mind power trying to hack a system will always be greater than that employed to design the system.

Therefore it would be logical to design any future system so that it can recover from a hack. It is more important that a system can recover from a hack. Trying to make a system hackerproof or indeed pirateproof is a futile exercise.

Of course the progress of electronics has a devastating effect on the security of systems. The operational lifetime, or more precisely, the hack free period of a system is now less than five years. It varies with the amount of hackers going after the system. Thus for a sporadically used system, there may be very little risk of the system being hacked. Of course for a widely used system, a hack is inevitable.

There are some people who would prefer that this version of the Black Book did not exist. They are scared of the fact that the systems that they claimed were invincible were anything but. In many respects it is a bit like the Emperor's new clothes.

A scrambling system is like a very high stakes poker game. If the channel is bluffing about its scrambling system then it will loose millions. Most of the systems that are coming on to the market are actually fairly secure. It is the small design flaws that allow them to be hacked.

The Black Book has become the "bible" of scrambling systems. It seems that the book is often consulted to find the characteristics of a scrambling system by those whose channel employs it. Apparently the manufacturers of the systems rarely supply interesting data sheets. Some manufacturers that I have heard of adopt the "Mushroom Strategy" with users of their scrambling systems. They keep them in the dark and feed them on crap. As with the previous version, any scrambling system that I could examine has been included. This also includes the hacks on particular systems.

Most of the information in the book still applies. Therefore where necessary I have left the original text in place. I have also expanded certain areas. The main problem for this volume of the Black Book was the vast amount of information available. It was more a question of what was important enough to be included.

Upgrades In This Version

The underlying principles of scrambling systems remain the same as does much of chapter two. Some the case studies have had to be revised as the channels using the systems have dropped them.

The data sheets have been improved and each system has been assigned a "McCormac Rating". The criteria for this rating system is explained in some detail. Essentially it defines the hackability of the

system. Many systems that were graded secure in the last version have now been hacked. The new McCormac Ratings reflect these events.

Many of the systems detailed in the third chapter of the previous version are not in use any more. There has been a gradual shift away from old analogue scrambling systems. Some analogue systems such as Discret and IRDETO are still in use throughout Europe. Even though some of the systems are not in use any more, the representative circuits for that system are left in place. These can often be applied to other designs and provide good references.

As in the previous versions, chapter four deals with audio scrambling systems. Though many of the systems featured are not as widely used as they used to be, there are still some who see a scrambled audio facility as a good thing. In the days just before publication, a report surfaced that Sky was working with a UK company to perfect a digital audio system that would connect via the SCART on the back of the decoder or IRD. The report stated that it was in prototype stage and was to be introduced in the event of the 09 card being hacked.

At the moment, it has not been possible to confirm this report of a digital audio dongle. It may not be even digital. Originally the VideoCrypt system was specified with a spectrum inversion audio scrambling system. It is unlikely that the audio scrambling facility is analogue though stranger things have happened.

Chapter five has been somewhat expanded. In case you haven't heard yet, Sky were beaten in court when they went to prosecute Satellite Decoding Systems for a copyright infringement of the program in the Sky smart card. The ramifications of the court case are examined in this chapter.

The information acquisition section deals with how hackers obtain information on scrambling systems. Much of the information on a system will be hidden in plain sight. Two of the best sources of information are the boasting businessman and the boasting engineer/technician. The businessman tends to provide a lot more information as it is easier to get classified information from someone who does not know it is classified. The techniques in this chapter are standard techniques used in every area of intelligence gathering whether for industrial espionage or State espionage.

Some of the techniques on obtaining information have been expanded. It appears that the bigger channels are the commonest victims of the methods. With publicity departments it is what is not said that is the most important thing. If these channels are to have a fighting chance, then the publicity departments must be trained in what not to say.

A number of dirty tricks that are in common use in counter-piracy operations are covered in this chapter. Some of these have been used by pirates against some of the parasites in the industry.

This section has been expanded to cover some of the information available on bulletin boards and other on-line systems. Much of the information is actually free.

Reverse Engineering is something that everybody does. Of course nobody admits to doing it. Reverse engineering is a fact of life in the electronics industry. Some companies who are victims of REVENGE work are actually stupid enough to complain about it. The reverse engineer is perhaps the most skilled type of engineer working in electronics. He has to be able to disassemble, understand and reassemble a circuit. The top revengers can reverse engineer a circuit without actually disassembling it. To the uninitiated, this seems like magic. It can also cause problems. When one revenger walked into a pirate laboratory, the technician hid the circuit board he was working on under the table. He had heard that the revenger could reverse engineer a board just by looking at it - something that wasn't totally false. This chapter will not turn you into such a paragon but it will teach you the basics.

The legal ramifications of reverse engineering are also covered in this chapter. There are a number of situations where it is possible to hack a system without having to resort to popping the chips. These situations are, surprisingly, legal. Much of this section deals with the events in the Irish High Court where Sky had to admit on the record that their system was hacked.

Cryptology and access control architectures are covered in chapter six. This chapter has been considerably expanded. The main emphasis is on the crypto-systems that have been used in scrambling systems. The DES and RSA algorithms are examined in detail.

The DES algorithm is used in VideoCipher II and EuroCypher. Of course EuroCypher has been consigned to oblivion. Perhaps the most startling discovery is that DES or rather an adaptation of it is used in

EuroCrypt-M. The main problem associated with the RSA algorithm appears to be the process of raising a number to a large power. A simple method of carrying out this operation is shown.

Over the last few years, the main emphasis in the Blackbox industry has been on hacking VideoCrypt. In the Irish court case, News Datacom claimed that they believed that they had developed a One Way Function. This claim was shot down in flames by an expert witness for the defence.

The concept of a one way function is examined in this chapter. The One Way Function in the VideoCrypt system is used to generate the decryption seed for the decoder from a thirty-two byte input. The actual hacker version of the VideoCrypt One Way Function is also included in this chapter.

The hacker version, known as the Ho Lee Fook algorithm, is simple and elegant. Of course it is also dangerously simple. Most hackers were expecting the algorithm to be extremely complex, perhaps even more so than that used in EuroCrypt-M. The reality was far different. So different, that many hackers found it hard to believe that it was that simple. One or two thought that News Datacom had pulled a fast one on the channels using their system. Truth should always have an elegant simplicity, except in signal security where it should be protected by a wilderness of mirrors.

The Fiat-Shamir Zero Knowledge Test may well have been used somewhere in the hierarchy of VideoCrypt but it does not appear to be used in the generation of the actual decryption seed generation. A full description of this algorithm is provided for informational purposes.

At the time of writing the 09 smart card is in operation by Sky. It has acquired the nickname of the "John Player Special" after a brand of cigarettes that it resembles. The 09 smart card is undergoing analysis and no doubt a long lasting hack will follow.

Chapter seven deals with video manipulative systems. A VMS is a system that digitally scrambles the video. Most of the newer systems use this approach. While it can be a more secure way of scrambling the signal it does not confer unhackability upon the system.

The MAC systems are covered in this chapter. The section on B-MAC has been considerably expanded and now contains the information on the American hacks. To date most of the hacks are

hook type hacks. The identity and key set of a valid decoder are inserted in another decoder to make it run as a virtual clone. A video only decoder is also a probability.

The VideoCrypt system is dealt with in some detail. It is one of the most widely used systems on satellite and as a result it is a major target. Despite an overwhelming abundance of pirate smart cards, certain people still would claim that VideoCrypt piracy problem is minor. Some of the older hacks have been countermeasured by Sky. Each of the hacks is examined and where necessary actual details of the hack are given.

The full details of the Ho Lee Fook, OMIGOD and DDT hacks are given in this chapter. This includes the full source code listings for each hack.

Other VMS such as VideoCrypt-S, VideoCrypt-2, Cryptovision and Nagravision Syster are dealt with. Of these, the VideoCrypt-S system has been somewhat of a failure for purely economic reasons. It is a good system but interfacing it to the off-air system and video recorders caused too many problems. The programming carried on the services did not have the take-up that the planners had envisaged.

The details on VideoCrypt-2 or VideoCrypt-Europe are still vague. It is a more recent and perhaps improved version of VideoCrypt. Its primary market is mainland Europe. Some of the VideoCrypt channels on ASTRA are already multiplexing the datastreams between Video-Crypt and VideoCrypt-2. This has caused problems such as long lock-up times on some of the older decoders.

Chapter eight covers both cable and MMDS security. Of course in the case of MMDS, security is not applicable unless there is a good scrambling system used on the net. Often there is no actual scrambling system employed. Some of the MMDS nets are still transmitting in the clear. Pirate downconverters are available but there seems to be little if any action to stop their distribution.

To date Ireland is the only country in Europe using MMDS. It is using the 2.5 GHz band. The UK has ideas about using an MMDS system operating in the region of 12 GHz though it remains to be seen if it will ever get into operation. Despite obvious cynicism, MMDS is proving to be successful in some areas in Ireland. In other areas it is creating divisions.

MMDS using 2.5 GHz was a fine system for the likes of Canada and the USA in the seventies. In the nineties it is a ridiculous antique in its present format. Add digital compression and it might be a usable system but its present format is a disaster for the Irish situation. Only some parts of Ireland are flat. With an MMDS system, the receiving site antenna must have a clear view of the transmitting antenna. With hills in the way this can be difficult. The local solution of rebeams is equally as antiquated though more acceptable to the local public.

Scrambling on cable and MMDS systems in Ireland seems to have been a failure. Where the scrambling system was employed for premium services only, the market penetration was pathetic. Then again the programming that passes for premium programming is not that good either. Blanket scrambling of cablenets has had more of an effect as it forced cable subscribers to get a descrambler or two.

The Cryptovision system is used for premium channel scrambling on the Cablelink nets in Ireland. The main premium channel attraction has been Sky Sports. Sky Movies and The Movie Channel find it very hard to compete against the video cassette rental business.

In Ireland the Jerrold Starcom system is used on the Cork cablenet. The Jerrold system is an antique in that it uses a scrambling technique that interferes with the synch pulses. In the United States, Radio Electronics magazine published a circuit diagram for a descrambler for this scrambling system. Naturally Jerrold were upset over this. Apparently they had set their legal lapdogs yelping. Apparently in the USA a bite from a pack of these shih-tzus can be financially painful.

Of course the printed media is not the only source of hacks on this system. More than a few computer BBS carry the actual ROM fixes for many cable systems. All you have to do is replace the official descrambler ROM with an EPROM containing the fix. Then you have full access to the programming on that cablenet.

It should be made clear that hacking or intercepting services in Ireland is illegal. This book may also be illegal as it examines the security of scrambling systems. The Irish Broadcasting Act 1990 is intended to limit if not eliminate cable and MMDS piracy. It can be applied to satellite piracy but requires a ministerial order. Basically the act will provide protection to any satellite television channel of Irish origin. If the state broadcaster decides to start a service via satellite then it would not be possible to supply pirate cards for the channel from Ireland.

To date there appears to have been no prosecutions for cable piracy as in actually hacking the scrambling system. The prosecutions that have occurred have been for patching into the cablenet without paying. The term used is "Self Connectors". You have got to wonder at the mind that dreamt that one up. On my local cablenet it has the word "Pirates" in brackets. Apparently the term "Self Connectors" originated in Dublin and since there are two countries in Ireland, Dublin and the rest of Ireland, it was obviously felt that a translation was necessary.

Chapter nine covers the relevant details and procedures of decoder connection. Some descrambler manufacturers have allowed the use of their data sheets.

An additional section now contains the information on smart cards. Smart cards are now an important part of the Blackbox industry. Therefore it was necessary to expand the information available. This section covers both memory cards and smart cards. The relevant technology of the various hacks is also covered.

Memory cards are commonly used in payphone applications. This might be seen as going off on a tangent from the subject of scrambling systems. Appearances can be deceptive.

There were some rumours that these cards would be used for special one-off events on various satellite scrambling systems. In terms of security, memory cards are not as secure as smart cards containing dedicated processors. The use of simple memory cards would be suicidal. There are of course other versions of the memory cards that are more of challenge to hack.

The problem is that most of the systems designed to work with the memory cards are designed to work with the EPROM types rather than the EEPROM versions. The 8052 in the VideoCrypt-I decoder has the routines to use EPROM cards instead of the smart cards. As a result there is an actual decoding algorithm in the decoder. However this algorithm is probably not as complex as the one in the 09 cards.

The Hacking Hall Of Infamy

The following is an examination of some of the mistakes and general screwups that have led to serious hacks. Many of them are due to non-technical people underestimating the risks that their systems faced. In some of the cases, it was not fault of the people involved. They either had not been properly briefed or had been briefed by JAFAs. Ignorance may not be a crime but it can be fatal.

VideoCipher Is Tamperproof And Undefeatable (sic)

Perhaps the stupidest and most ignorant statement ever made about a scrambling system was made in 1986 about VideoCipher. Specifically VideoCipher II, the planet's most hacked system.

"The VideoCipher system is a very sophisticated system, tamper-proof and undefeatable." Naturally this quotation came from a marketing person. Now what was unbelievable about this quotation was that there was a confirmed hack on the system in June 1986. Apparently the news had not reached VideoCipher.

BBC Vs Hi-Tech

In the UK, piracy has been highlighted by a number of cases, the most notable being the Hi-Tech XtraVision case. The BBC attempted to stop the UK descrambler manufacturer, Hi-Tech XtraVision manufacturing and selling descramblers for the BBC Europe service via Intelsat VA-F11 at 27.5 West. The original ruling on the case stated that the UK Copyright Patents And Designs Act 1988 was not usable in the case as it was badly framed. The end user of the descrambler was outside UK jurisdiction and so UK law was not applicable. It was overturned on appeal and Hi-Tech XtraVision decided not to defend.

BBC Pressures Elektor Electronics

A stupid event occurred earlier in 1990 involving the "Elektor Electronics" Magazine. In the February 1990 issue, this magazine published the first of a two part constructional article for a SAVE descrambler that did not use crystals. The decision to print was taken when the first ruling in the Hi-Tech XtraVision case was in force. The BBC lawyers then saw the magazine and got upset and threatened Elektor. Elektor pulled the March 1990 edition of the magazine. The full circuit diagram and theoretical description was already in the hands of

those who wanted it. Any hacker worth his salt can design a printed circuit board. It makes the lawyers and the BBC look like utter idiots. They took action after the event occurred and thus drew the matter to the attention of the media. It is not surprising that hackers consider some lawyers as being between rocks and bacteria on the evolutionary scale.

This situation was badly handled. If the BBC and their lawyers had remained silent, then the descrambler design would not have had as great an effect. Elektor later published a design for an audio descrambler that was capable of being used on this system. Very few people actually knew what the design was. It is not known if the BBC and their lawyers actually knew what was going on.

FilmNet Helps The Hackers

The system owners almost always hold back at least two further scrambling levels until the system has been in use for at least six months. This is a good tactic as a lot of the inexperienced hackers will be caught out when the further level of scrambling is introduced. It is also an unwritten rule that the level will be introduced at a time that will cause maximum damage to the professional hackers.

The best example of this tactic was Filmnet's introduction of a further level of scrambling three days before the 1987 Cable And Satellite Show. This left a lot of dealers with egg on their faces as they were selling pirate descramblers that did not work. Fortunately for some dealers, the three days were enough to update their demonstration decoders. Filmnet should have introduced the further level during the show for maximum effect.

The show was, in counter-piracy terms, FilmNet's biggest disaster. A business person representing FilmNet was boasting about how they had faked out the hackers. The fact that FilmNet had thirty one possible variations to play with was mentioned. Unfortunately one of the people who overheard was a hacker.

The FilmNet representative was unfamiliar with binary. In binary, 0 is also considered as it is a logical state whereas to the businessman it means nothing. In technical terms, Filmnet has five possible levels of encryption and thirty two combinations. Since level zero is clear this leaves thirty one possible variations. This effectively condemned FilmNet to four years of being totally hacked.

Sky Advertises Pirate Descramblers

In late 1990, strange adverts started to appear in the UK satellite television press about the fact that FilmNet decoders were illegal. Other scare tactics claimed that the decoders would soon be obsolete. There were rumours that Sky were tied in to this advertising campaign. On the Dealer Text teletext service on Sky News, (teletext page 830), the evils of pirate FilmNet decoder were proclaimed.

On teletext page 491 on Eurosport, there was an actual advert for pirate FilmNet decoders. This was rather embarrassing for Sky. Once they found out about the advert, they quickly removed the FilmNet reference.

Sky, at that time had control over Eurosport. The teletext magazine was assembled by Sky but unfortunately they did not adequately screen the advertisements.

Sky Markets Do It Yourself Piracy Kit

Perhaps the stupidest event in counter-piracy history was perpetrated by Sky's marketing people. Evidently Sky's counter-piracy people were not consulted on this. If they had been they would have stopped the scheme dead in its tracks. Perhaps the reason was that Sky did not have anyone who could be classified as being involved in counter piracy.

In 1990, Sky was locked in battle with BSB. Sky was trying to hook as many viewers as possible for the fledgling Sky Movies. Then some utter nutter of a marketing genius struck. The scheme was that Sky would give three months free viewing of Sky Movies to purchasers of IRDs.

The fully active smart cards were bundled with the IRDs. Included in the packet was a subscription form for Sky Movies. The logic was that typical of business school text books. It totally ignored the real world.

The smart cards never reached the purchasers of the IRDs. Instead, they were shipped to mainland Europe where they were sold for high profits. Often dealers would forget to mention the free viewing cards to purchasers of IRDs in the UK and Ireland. Many of the purchasers were ignorant of the scheme anyway.

In European magazines, adverts appeared for decoders and smart cards. Sky had people trying to track down the sources of the companies advertising. This was an essentially futile operation. Sky had actually caused the piracy problem. What was unnerving was the sheer naivete of those Sky people involved. They actually believed that pirates and hackers would play by their rules.

Sky - The Most Pirateproof System

Marshall McLuhan's image of the Global Village is a strong one. So is the image of the village idiot. In the days when analogue systems were the norm, FilmNet was the laughing stock. Their system offered little challenge and whatever they tried, the hackers countered it. Sky ran little sanctimonious messages on their teletext service pointing out that the piracy on FilmNet would soon cease when FilmNet introduced new countermeasures.

Now the mantle of the village idiot has been passed to Sky. Their actions after the first quarter of 1993 were anything but clever. In fact their actions were more akin to that of a headless chicken.

In March of 1993, Sky decided to destroy their security department. Ken Crouch, the head of Sky's security department had gained respect among hackers. For a few years he had more or less kept Sky from serious harm. He limited the effects of any hack to such an extent that he had a hack named after him.

Apparently Ken Crouch was doing too good a job. As Sky had not suffered any serious hacks for a few months, some idiot or idiots in Sky incorrectly perceived the situation. The hackers had been defeated and therefore the security department was not necessary.

Sky's VideoCrypt was once more invincible. Their publicity did proclaim it as the most pirateproof system yet devised. Ironically they had fallen victim to their own stupid claims. Just because their system was temporarily secure, they fell into the trap of thinking that no hackers were working on hacking it.

By April of 1993, the first versions of the Ho Lee Fook hack leaked on to the market. The first versions were based on the 8752 chip. This is the EPROM version of the 8052 as used in the VideoCrypt decoder. The Ho Lee Fook chip was meant to replace the official 8052 chip in the official decoder. The name for the hack summed up the general reaction of people when told of the hack.

The 8752 version was too insecure. The hackers were too used to popping these chips. The expertise in popping these chips came mainly from the FilmNet, Teleclub and RTL-V pirate decoder operations. The later versions of these pirate decoders used 8751 and 8752 microcontrollers. Good designs and programs were copied. The first of the 8752 Ho Lee Fook chips were probably copied as well.

The 8752 chip were not cheap but the cost and availability was causing problems. Though the implementation of the hack was elegant, installation was not. It was downright messy. The decoder had to have the original 8052 chip removed. A chip socket had to be soldered in its place. Then the 8752 could be inserted. It was messy, time consuming and expensive. A cheaper alternative was needed.

That cheaper alternative came in the form of the PIC16C54. This chip was low cost in quantity and extremely powerful. It used a different architecture and instruction set to the VideoCrypt card. It had only 512 bytes of EPROM. Significantly less than that in Sky's own cards.

Soon the pirate cards with PIC chips were in mass production. The cost was low enough to make them disposable technology. When ever Sky implemented an upgrade the cards were returned to the dealers who replaced them with a new card.

The PIC16C54 EPROM and One Time Programmable versions were replaced by the PIC16C84 version. This move was the most dangerous for Sky and News Datacom. The pirate cards could now be updated at a rate that probably exceeded the update rate of Sky's own cards. It was merely a question of returning the card to the dealer. The dealer would then plug the card into a programmer attached to a personal computer. The computer had a modem. As soon as there was an upgrade to Sky's Electronic Counter Measure, (ECM), it was available over the telephone lines.

At the time of writing the Ho Lee Fook hack is still in operation on the older implementations of the VideoCrypt system such as that used by The Adult Channel. The introduction of the 09 card issue has caused some problems but it looks like it will be hacked.

When Sky introduced their system, the smart card was seen as the ultimate and very final cure for piracy. No longer would channels have to worry about hackers ever again. At the time, a lot of people fell for this propaganda. Sky's publicity department worked hard to have this official viewpoint accepted.

Naturally some of the rent-a quote reporters fell for this viewpoint. The generous reason being that they had no technical knowledge on which to base their judgments. The few of us with technical backgrounds were very suspicious of Sky's propaganda.

It had all of the classic hallmarks of the implementation of a mediocre scrambling system. The potential for updating was stressed. A famous expert was wheeled on as the architect of the security algorithms.

Of course it remains to be seen if they will make such stupid claims for the 09 smart card issue. There is at least one unconfirmed report that a Sky employee was overheard in a pub claiming that this time Professor Adi Shamir had come up with a solution that would knock out all of the pirate cards. Now where have we heard that before?

What Is A Hacker?

In the last few years there has been a virtual deluge of books on hackers and hacking. Even movies were based on the subject. The electronic hacker requires a greater knowledge base than a computer hacker. It requires a working knowledge of computing and a good knowledge of electronics. Indeed there has been an influx of computer hackers to the ranks of electronic hackers. My comments in the previous versions are still applicable as they relate to the electronic hacker rather than the computer hacker.

At this point in time there are perhaps more computer orientated hackers than purely electronic hackers. This is due to the huge influx of computer hackers into the business. Cracking Sky's codes is now a major pastime in many colleges and universities. The sheer mass of mindpower and computer resources now deployed against VideoCrypt makes future hacks on the system inevitable.

Many of the books on computer hacking seek to, and in some cases actually do, identify the main traits of hackers. Indeed some of them such as "The New Hacker's Dictionary" do an excellent job. Electronic hackers are more difficult to quantify. I do not think that anyone has actually tried to properly define what an electronic hacker is.

As Electronic hackers are rarer than computer hackers, this is an exceedingly difficult thing to do. As an electronic hacker, I am in a better position to comment on the main traits required for this type of hacking. Much of the comments that follow apply equally to computer hackers. These comments may be offensive to some of the pseudo-intellectual sociologists reading this.

There is no such thing as an average hacker. A hacker by nature will be above average intelligence. Out-thinking is a pastime that generally restricted to those with above average intelligence. Since the level of electronic knowledge required for hacking is high this would tend to restrict hacking as a hobby to technicians and engineers or at the least a person with a good knowledge of electronics.

Another interesting aspect in hacking is that all of the top electronic hackers and most of the average electronic hackers in Europe are male. This is not a surprising thing. Advanced hacking requires phenomenal visio-spatial abilities and the ability to grasp complex and extremely abstract concepts. These are specifically male traits. Any feminists reading this may be offended. Don't blame me, blame God. He designed the Human race.

There appears to be one common factor in the background of electronic hackers - an interest in electronics prior to third level education. Some hackers look down on engineers as blow-ins. The majority of engineers only decided to do engineering on entering third level education. Or in some cases their parents made the decision for them. For some of them engineering is only a job. They probably did well in exams all throughout their academic careers because they could memorise some fact or text and regurgitate it on an exam paper. An electronic hacker will have a fascination with electronics and it is this fascination with electronics that these paper engineers lack. Luckily these paper engineers do not last very long in electronics and find other positions that suit them. In the early eighties, one paper engineer told me that it was impossible for a mere mortal such as myself to design a satellite receiver system. He also said that satellite television was never going to be used on a widespread basis. The chap now sells shirts for a living!

As the electronic hacker has had previous experience in electronics, they will not do well in third level education. Most will drop out of their course because they become bored with what they are being taught. In this respect, the above average intelligence of the hacker is a disadvantage. Most of the third level courses in electronics will be like a mental straight jacket to the hacker. Most non-hacker readers will automatically think that just because a hacker has above average intelligence he will just get on with the course. Unfortunately it is never as simple as this. The average academic year is thirty-six weeks long. If you could complete this course in three weeks would you hang around for the other thirty three weeks?

There are probably readers who think that hacking is a crime in the sense that it is theft of service. The legislation varies from country to country. Some countries in Europe, such as France and Ireland have rather draconian laws against piracy.

As the moral kind of reader regards hacking as a crime, he or she may not try to hack. The attitude of a hacker is totally different. A hacker would generally know that hacking is a form of theft of service but would not really be too concerned. The moral and ethical conditioning that society imposes has a greater effect on those with average intelligence, after all the morals and ethics are generally created by those of average intelligence. When one is of above average intelligence, there is often a feeling of not belonging. This feeling of not belonging results in a sort of intellectual arrogance where the individual concerned decides that the normal morals and ethics do not apply to him as he is not normal. This is of course an extreme example but a milder form of this decision would explain the attitude of most hackers to the moral aspect of hacking. The vast majority of hacking is for fun. When hacking is executed for money, the moral and ethical aspects are suspended. All's fair in love, war and business.

In my opinion, anyone involved in hacking for purely experimental reasons should not be prosecuted. It is disgusting that people who are often critical thinking addicts or at least are not involved anything creative, should decide to hassle experimenters. (This of course excludes criminal lawyers who are among the most creative experimenters known.) These people do not apparently recognise that all of the major inventions were made by experimenters and if it wasn't for experimenters Humanity would still be swamp slime.

On some of the computer bulletin boards, the good and evil of experimental hacking has been debated. The most often proposed argument on the evil of experimental hacking is that it is shop lifting in a different guise. I do not agree with this. It is, to use another analogy oft quoted by anti-hackers, like saying that guns kill people. The logic is flawed.

Incidentally guns do not kill people, bullets do. The whole objective puter program reverse engineering. The aim is to stop the reversing and analysis of computer programs. This has parallels with the Blackbox industry. It is unfortunate that those who try to make the laws that govern technology are those who are generally least suited to the task. Hackers, engineers and programmers thrive on the free exchange of ideas and information. The law, it seems, would try to regulate this flow of information.

The law is often a few hundred years out of date. Judges are, in some European countries, allowed to serve beyond their sell by date. To expect them to cope with extremely complex technological nuances is a bit much. However lawyers are generally fast learners so they can comprehend the concepts when they are explained to them in simple analogies. Perhaps by an extreme suspension of disbelief, they are also hackers in that they use, adapt and draw conclusions from information.

It is generally their task of these lawyers and consultants to crush complex technological thoughts into mental baby food, or in layman's terms; plain English, in the rare cases that actually come to trial. Of course it must be a terrifying experience when in the middle of a case on computer software, the judge asks what software is. Such a thing allegedly happened in the UK a few years ago.

Where legislation exists to cover hacking, it is usually of the blunderbuss variety. It can be used to cover every eventuality. Often this legislation is introduced at the behest of interested parties. In this manner it reflects much of the law in that its aim is the perpetuation of those involved in its use.

For example in Ireland, the Broadcasting Act of 1990 was intended to protect cable companies and MMDS operators. Now just who was the biggest cable company at that time? Cablelink of course. Cablelink was owned primarily by the state via a semi-state operator or two. The state emphasis on the legislation can be seen in the structure of the

act. The Act does not cover foreign satellite borne transmissions without a statutory instrument signed by the minister for communications.

There is a trend nowadays to rely less on the law and more on secrecy. A company will not patent a new system because it supplies a ready source of information for hackers. This is perhaps a more sensible approach. There is an aspect of law where a system could be declared a trade secret. Some would argue that this offers enough protection. To someone abiding by ordinary rules it would. Hackers do not abide by such rules and the concept breaches one of the prime rules of secrecy - the fewer who know the better the secrecy.

The problem with many of the access control systems is that much of the algorithms are often direct implementations of public domain material. Sometimes to make things a little more difficult for the hackers, these algorithms might be tweaked. This can of course result in some very dangerous situations if the manufacturer ever decided to protect the system in court.

Perhaps the lesson of secrecy has been lost on executives in scrambling system manufacturing companies. The first thing to do when considering the algorithms at the heart of a system is to make sure they are indeed secret and have not been published in a paper in some journal or book. Algorithms are not copyrightable in the European Community. However in the USA for some strange reason they are copyrightable.

The use of the law in counter-piracy is like a loaded musket. It is useful against a single opponent, which by some accident could be you. In piracy, a system will be attacked from hundreds of directions. In some countries, the UK for instance, the relevant law provides for statutory conviction. It would not be feasible to prosecute all the attackers. Some may not have the money to pay the fines. An indiscriminate approach would lose the battle for the hearts and minds of the users. If potential subscribers see the channel as an oppressor of the man in the street then they are far more likely to opt for a pirate decoder or card.

Despite all of this there are still some channel executives who think that legal methods can be used to stop piracy and or hacking. These executives are not technical. Commonly they are products of a business or legalistic education. Generally they lose this attitude after actually having some hands-on real time experience.

Hacking is an essential item in the evolution of technology. It stretches the technology to the limits and then goes one step beyond. Many of the advances have been made by hackers. Some top professional hackers were among those who were experimenting with satellite in its early days.

Divergence Or Convergence?

The term "convergence" is a buzz word much in favour with the marketing people. The concept is that all of the transmission media are coming together. Things in the real world are slightly less clear.

For the Blackbox industry, the strategy of "United We Stand - Divided We Fall" has been a recipe for disaster. In the business of scrambling systems, the more variety the less risk there is that a single hack will have a widespread effect. It is more a case of compartmentalised risk. Even after all the scrambling systems failures of the last few years, there are still idiots who believe in a single encryption system. Again real time experience is sadly lacking among them.

It would be easy to apply the rules of evolution to this situation. Put simply, it will be the survival of the fittest. The system that can adapt and cope with hacking and the market demands will be the survivor. If a system is considered as a species, then it must continue to evolve and adapt to its environment. If it remains static then it becomes extinct.

The scrambling systems of the past few years are moving towards a non-static or fluid architecture. The smart card was evidence of this. In the event of a hack on the system, the smart card could be replaced. Of course the theory of the detachable secure processor has been dealt a cruel blow by economics. If the number of cards being used on a particular system becomes too large then replacing them may be prohibitive.

Take Sky's predicament for example. They have an estimated three million subscribers. Now if some two million of those subscribers have to get new cards again, it would mean a cost of approximately ten pounds per subscriber. Twenty million pounds is a lot of money for a channel to spend every time it has to upgrade its cards. As a result Sky and News Datacom are trying everything to stop the Ho Lee Fook Version 2 cards from working.

Some channel executives regard piracy as a form of disease. For some of them it is a simple emotional response without any deep underlying logic. Strangely the concept of piracy as a disease or virus is a good one and perhaps a very accurate one. It also ties in nicely with the theory of evolution as applied to scrambling systems.

If a hack is considered as a virus then the countermeasure is effectively the cure. Over a period a system will, like a biological system or organism, build up a defence against various types of hacks. This would come about as the various countermeasures are added to the system's datastream.

If there is some diversity in the implementation of the system then some of the hacks would only affect a few implementations. Of course there is always the potential for a Holy Grail hack. Such a hack would bring the system crashing down regardless of the differences between implementations. In Human, terms it would have the same potential as Rabies. Except in this case only the executives of the hacked channels and system manufacturers foam at the mouth.

Of course there are other factors involved here. A successful virus does not kill its host immediately. If it did so, then it could not spread and would die out. This is perhaps the self-defeating aspect of the Holy Grail hack. It is a victim of its own success. The channels using the hacked system will have their main fee gathering mechanism destroyed. As a result they may not survive.

The Ho Lee Fook hack can be classified as a Holy Grail hack. To date it has affected all of the major implementations of VideoCrypt in Europe. It may soon be affecting the other implementations of VideoCrypt elsewhere on the planet. Sky in New Zealand, Star TV in Hong Kong and DirecTV in the USA are potential casualties.

The Card Tricks hack on D2-MAC EuroCrypt-M is similarly a Holy Grail hack. While this system has far more potential than VideoCrypt it has a fatal flaw. It is a committee designed system. A large amount of technical detail is openly available on this system. This fact alone gave hackers a very good insight into the operation of the system and led, eventually, to the hack.

Of course the EuroCrypt-M system is more complex in implementation and security than VideoCrypt. When you read the EuroCrypt specification document, it is easy to appreciate the complexity and elegance of the system. There are many more possibilities for this system and as such it is perhaps more resilient in terms of hacking.

Like VideoCrypt, the EuroCrypt-M system is smart card based. The main action that the users of the EuroCrypt-M system have taken against the hackers are mainly electronic countermeasures. These have been marginally successful. The hackers generally had solutions within a few hours though sometimes it can take a few weeks.

Some rather naieve people have claimed that when digital television arrives hackers will disappear because it will be too difficult to hack. Yeah right! The same people, or their predecessors said the same thing about smart cards and VideoCrypt. The same people believe in unbreakable codes and publicity brochures.

Digital television is only a medium. What will protect the signals is the security overlay. If this overlay is insecure then it will be hacked. For example, the VideoGuard system is the pay television security overlay developed by News Datacom. The analogue implementation is called VideoCrypt. A different implementation is used to provide the security on the DirecTv system in the USA.

In its analogue form the VideoGuard system has been compromised. The security on the DirecTv system is still an unknown factor. According to the first information from the USA, the smart card will have to be left in the decoder continually. Some sources have stated in magazine articles that the smart card for the DirecTv system is better than that employed on the VideoCrypt system. It is also supposed to have more resident algorithms and be more updatable than the VideoCrypt version. Of course this could be true or it may be a rationalisation designed to avoid tricky questions. Given the knowledge base here in Europe, DirecTv will be in very severe trouble if the main part of the security overlay has not been totally overhauled.

Other digital television systems are also under development. What may well occur is some form of standards battle like that of VHS and Betamax. In either case the security of the system may be the factor that decides the battle.

At this point in time it is very hard to believe in such a thing as a totally secure system. The purposes of a scrambling system are to prevent all but the most elegant of hacks and limit the effects of that most elegant of hacks - the Holy Grail.

This simple lesson of scrambling system design has been ignored once too often. Publicity brochures are filled with inane claims that the manufacturing company are pro-actively involved maintaining the

security of the system. Such claims are generally only the product of a marketing meeting. What they are really trying to say is that they cannot guarantee the security of their system.

It is impossible for any scrambling system manufacturer to truthfully guarantee his system. To do so would rule out any future development or discovery. Of course the marketing and PR people have to have some little bit of prestidigitation for the poor fools about to buy the system.

Most of the problems that Sky and News Datacom are suffering are due to their ignorant arrogance. It looked to the Blackbox industry like they had disregarded the power of the industry. Above all it seemed as if they regarded hackers as ignorant low lifes. A bad and fatal move.

The industry showed no mercy to Sky and News Datacom. Of course the way Sky and News Datacom handled the whole situation contributed to the problem. For all intents and purposes they were treating it like a case of corporate pilfering. When they had what they believed was enough evidence they went to law.

Sky and News Datacom could not implement any more decent countermeasures on the 07 card's datastream. As a direct result of this they have had to go for a new card issue. Perhaps if they had kept their security department and fired the accountants things might have turned out differently.

In Europe, we are now in a situation where all of the pay channels' scrambling systems appear to have been hacked. Yes there is even a rumour of a hack on Nagravision. In the United States and Canada, VideoCipher still has problems. The main difference is that piracy of VideoCipher is completely illegal. In Europe, there is no such thing as the blanket illegality of piracy.

In a somewhat romantic rationalisation, hacking could be the last vestige of a free society. In the USA, the government is trying to impose the Clipper chip on the public. It seems to be a part of a general move towards a big brother situation where there are no secrets from the government and cryptography is controlled. The rumblings of similar actions here in Europe have already been heard.

It looks like some politicians would like to control what we say and think just as some idiots in the broadcasting industry think that there should be a single unified scrambling system.

Fools try to control chaos and in the end the chaos consumes them. It looks like those who would impose such restraints on privacy do not appreciate the long term effects of their actions.

A single system only requires a single hack. From that point on, everything looks to be a rearguard action. While the hack may not occur immediately, it will occur.

The more protected something is - the more of challenge it is. When a system is portrayed as being impossible to hack, every hacker believes that it is only a temporary impossibility. Perhaps it is this sheer optimism that allies hackers with addictive gamblers. We all believe in, and often depend on, luck.

Almost invariably this belief in luck pays off. Systems are hacked because someone overestimates the security of a component or, as is more frequently the case, someone makes a mistake.

The players change but the game remains the same. It is stupid to claim that piracy will be eliminated, for if there was no crime then there would be no need for a police force and we'd all be vegetarian troglodytes. This is the real world - wake up and smell the coffee!

The Principles Of Security

Information is the most valuable weapon in the arsenal of a hacker. With knowledge of all previous systems, a new system can be quickly cross-checked and identified. Of most import, the weaknesses of the system can be detected.

All hackers tend to amass a rather untidy collection of magazine articles, notes and manufacturer's brochures. Very few hackers are over-enthusiastic about having everything filed away under relevant titles. In fact most of us tend to prefer the stable chaos system of filing.

The stable chaos system of filing is where things are dumped in piles. Since the locations of the piles are governed by fuzzy logic, (as used by the mind), it is easier to locate some article that you read five years ago. Of course this is one hell of an excuse to use when some one accuses you of being untidy. It is so improbable that it is perfectly plausible and perhaps true.

The following few paragraphs and diagrams are definitions of the basic video scrambling facilities. Most of the simple scrambling systems will use one or more of these facilities.

Once you are familiar with the facilities, you will be able to identify a particular scrambling system based on the presence or absence of these facilities. The more recent digital video techniques are also defined. These techniques can be more difficult to individually identify.

Many system manufacturers do not patent their systems for obvious reasons. As a direct result of this, some people will try to patent everything especially in America. Many of the people involved in designing systems do not like this approach. Instead they opt for the trade secret approach. One very important point to note about patents is that while the system principles may be described, the descrambling process may not be the actual one used.

Case studies of the various scrambling systems are used to illustrate the applications and weaknesses of the techniques. In this version of the Black Book, some of the case studies have been revised.

Synch Manipulative Systems

A Synch Manipulative System interferes with the synch pulses in the signal. The aim of such a system is to prevent the television receiver from locking up the picture. Most of the techniques are rather primitive when compared to digital video techniques but nevertheless they are effective. The weakness in a synch manipulative system is that they tend to leave the colour burst alone. While it is true that the colour burst is often voltage shifted with respect to the video, the actual timing is the same. It is therefore possible to hack the system by locking a synch generator with the colour burst.

Synch suppression is a relatively old scrambling technique. It is rarely used on its own. The horizontal synch pulse or horizontal blanking area is pushed in the video region of the signal. There are two accepted formats for synch suppression; pulse gated and sine wave.

Pulse Gated Synch Suppression

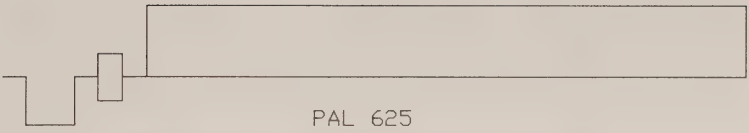
A pulse gated synch suppression system requires a pulse train phased with the scrambled signal for descrambling. The pulse train is used to control a "pull down" circuit that restores the horizontal blanking intervals or synch pulses to the correct levels.

The pulse train or recovery signal for the scrambled signal is generally transmitted on a separate subcarrier as in the FilmNet case. With the FilmNet Matsushita SATPAC system a composite synch signal was transmitted on a subcarrier at 7.56 MHz. On the cable version of the scrambling system, the composite synch signal is amplitude modulated onto the FM audio subcarrier.

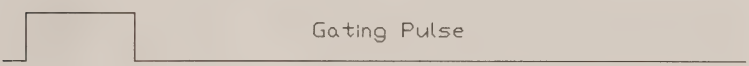
Sine Wave Synch Suppression

Sine wave synch suppression uses a sine wave to push the synch signals into the active video region. The frequency of the sine wave can be line frequency or a multiple of line frequency as in the Sat Tel SAVE system.

The descrambling of a sine wave scrambled signal is not as straight forward as the pulse gated system. The sine wave may or may not be transmitted with the signal. On some of the cable systems, the



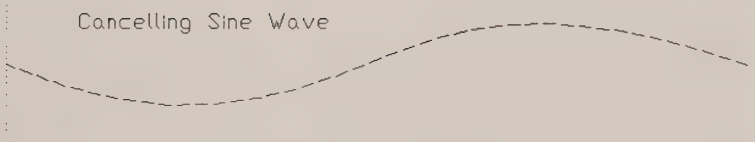
PAL 625



Gating Pulse

Pulse Synch Suppression

Sine Wave Synch Suppression



Cancelling Sine Wave

recovery sine wave is transmitted in an amplitude modulated format on the FM audio subcarrier. This method of descrambling is not exactly feasible on satellite. The most common method used on satellite is regeneration. The sine wave is stripped from the scrambled video signal and sent to a phase locked loop. The PLL is generally running at a high multiple of the sine wave frequency. In the SAVE system, the frequency of the interfering sine wave is approximately six times line frequency, (93.750 KHz). The PLL in the descrambler runs at sixty four times the sine wave frequency, (approx 6.0 MHz).

Synch Removal And Replacement

The removal of the horizontal or vertical synchs is an effective if rather insecure method of scrambling a video signal. Since the television receiver has no synch signal it cannot lock the picture. The colour burst is generally used by descramblers for lockup. The timing of the colour burst is rarely changed.

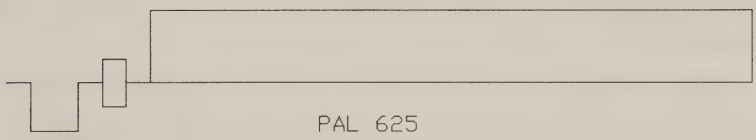
The replacement of the synch pulses with digital data is the commonest use of this scrambling facility. It is used in the OAK Orion system and the LuxCrypt systems. Digital data and audio blocks are used instead of the synch pulses. In the Orion system, a 2.5 MHz synch burst is transmitted prior to the data. This provides a lockup for the synch generators in the descramblers. The pirate descramblers used the synch burst to recreate the synch signals using monostables and simple PLLs.

Synch Inversion

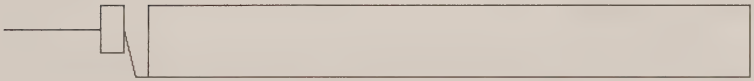
Synch inversion is a particularly nasty form of scrambling. Most of the polarity detection circuitry in pirate descramblers is geared towards complete line inversion. With this facility, only the blanking or synch section of the signal is inverted. The facility would optimally be used in a pulse gated system where the synch is suppressed.

Since polarity detection circuitry detects the difference between the horizontal synch pulse and horizontal blanking, the video polarity is judged by these levels. The FilmNet SATPAC system used this weakness in the pirate descramblers to their advantage. They inserted a peak voltage in the horizontal synch pulse so that the pirate descramblers could not interpret the polarity of the video.

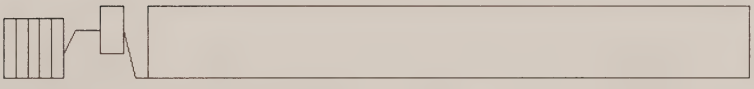
Synch Removal And Replacement



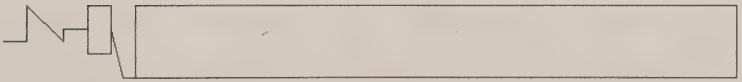
PAL 625



Synch Removal (Rare)



Synch Replaced With Data (Common)



Synch Replaced With Non Standard Pulse (Rare)

Video Inversion

Video inversion is perhaps the most widely used facility. It can be applied to gated, sine suppressed or normal signals. It can be tricky in application as the level of the descrambled polarities may differ by a few millivolts. This means that either a key must be included in the scrambled video or a balance potentiometer must be included in the descrambler.

A key takes the form of a section of the horizontal blanking level that is inverted with the video. In the scrambled signal, the horizontal blanking level will appear at approximately half video. With the video range being approximately 700 mV this half video point would be 350 mV. This provides the descrambler with a reference level on the descrambled line. The key can be sampled and compared with the normal polarity key.

This method of scrambling is more common on satellite based systems. It is not really suitable for terrestrial or cable based systems.

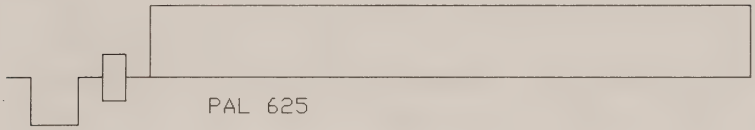
Field Inversion

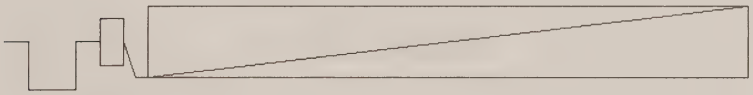
This is one of the simplest methods to implement and naturally the easiest to hack. One complete field of video, including field synch is inverted. The following field is normal polarity. Other sequences such as 1 normal and 3 invert can be derived from some flip-flops and a bit of combinational logic. It can be applied to the video only or the complete field. The inversion point is often half way through one of the lines in the VBI as opposed to the beginning or end of the field synch.

Line Inversion

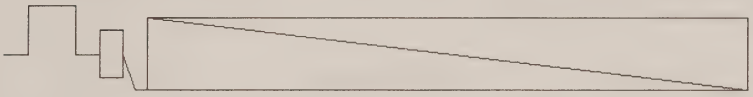
Line based inversion comes in two basic forms; Keyed And Nokey. The keyed inversion contains a polarity indicator in the line blanking. This is commonly used in systems like Oak ORION or LuxCrypt. This is the least secure form. The nokey video inversion is a more secure form. There is no indicator as to the exact polarity of the video information. The inversion sequence can be sequential or pseudo random. Due to the difficulty of establishing the black level in descramblers, the Keyed inversion is the commonest.

Line Inversion



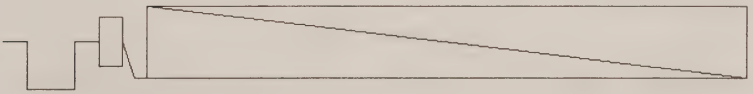


Normal Polarity Line. Synch Suppressed.

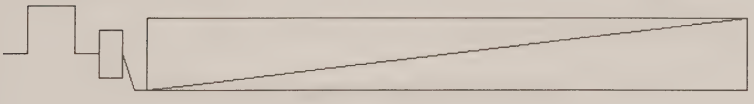


Inverse Polarity Line. Synch Suppressed.

Synch Only Or Video Only Inversion



Video Only Inversion. The suppressed synch is normal polarity. The video section is inverted.



Synch Only Inversion. The suppressed synch is inverted and the video polarity is normal.

Note: The terms Video Only Inversion and Synch Only Inversion can mean the same thing when applied to a synch suppressed system. On a clean synch system, Video Only Inversion is the only inversion type permitted.

The actual inversion sequence can be line based or field based.

Average Peak Level Inversion

Average Peak Level inversion, pronounced 'apple', is a more secure method of effecting video inversion. The polarity of the video is decided by the amount of black or white in a scene. Each frame is sampled and when the cumulative value of the samples exceeds a preset threshold the video is inverted. It does not change polarity again until the threshold is exceeded.

Video Delay

The video delay form of scrambling is used in a number of scrambling systems. The Discret system as used by Canal Plus is based on this system. The B-MAC system by Scientific Atlanta also uses this scrambling method.

Fixed Delay

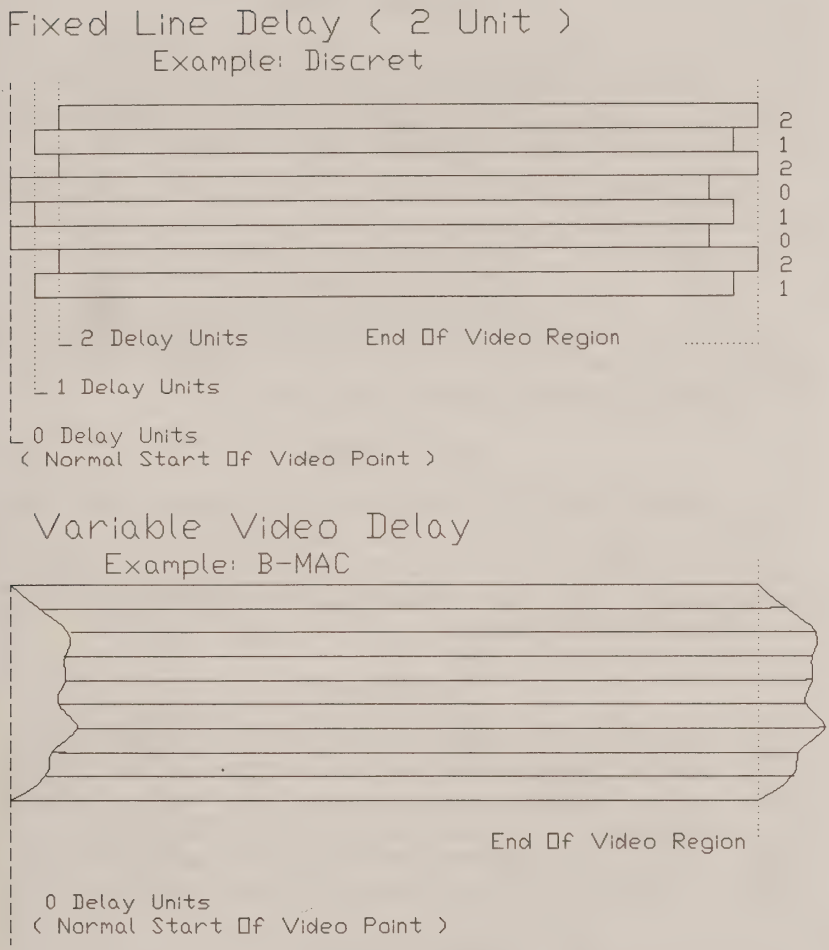
The fixed delay facility delays the video on each line by one of a number of fixed delays. In the Discret system, the delays are 0, 902 nS and 1804 nS. The delay can be implemented by CCDs, glass delay lines or gyrator delay lines. Once the length of the delay lines are known, the system is easily hacked.

Variable Delay

The variable delay is a lot harder to hack. In the B-MAC system the video sections of the line are delayed by varying the length of the data block. Again it is a question of ascertaining the minimal delay length and the maximum number of delay units. Off the shelf solutions can be more difficult to find in this type of scrambling system.

Video Position Modulation

This is the Macrovision PhaseKrypt system. It is one of the hardest systems to hack. It is a very secure method of video scrambling. The position of the video in the line is modulated. The video information itself is slightly shortened to accommodate this. The delay section at the end and beginning of each video area are filled with electronically stretched video. The delay is too slight to be properly detected and as a result it is extremely difficult to hack using a video only approach.



Note: In a Fixed Video Delay system, the video always remains in the confines of the video region. The positions of the synchs are unchanged. In a Variable Video Delay system, the video does not have to remain in the confines of the video region. It can enter the area that would be occupied by the synch of the next line. This makes it usable with MAC systems rather than PAL or SECAM.

Digital Video

The following techniques are generally applied to digitised video signals. Systems employing these facilities are generally harder to hack and in most cases the scrambling process is not actually hacked. The weak point is almost invariably the control circuitry.

In general these systems are complex. Chapter 7 deals in detail with digital video systems.

Cut And Invert

The digitised line is cut at a particular point and all data following that point is inverted. This can be achieved in analogue technology but there tends to be residual problems such as tilt.

Cut And Rotate

The digitised line is cut at a particular point and the two sections are rotated so that the last section becomes the first and vice versa. It is a rather secure method but the cut points have to be masked to prevent weakness and noise. The VideoCrypt system uses this form of scrambling as does Cryptovision.

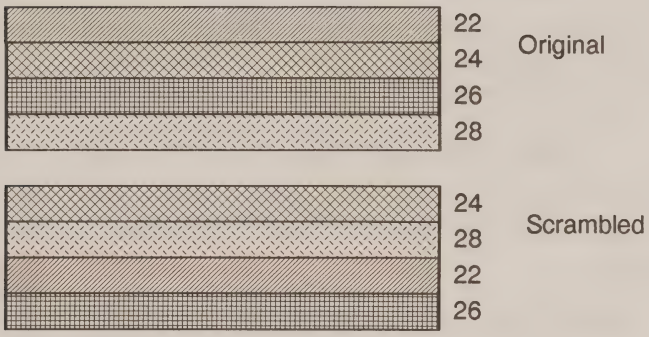
Line Shuffle

This system is purely a digital one. The actual field position of each line is changed. For example, line 26 might become line 38. The system can be applied on a field or frame basis. This is a memory intensive application and smaller line counts are generally employed. There is a rather nasty enhancement known as the sliding bar shuffle. This facility does not use a fixed dimension or fixed position shuffle.

Hard Encryption

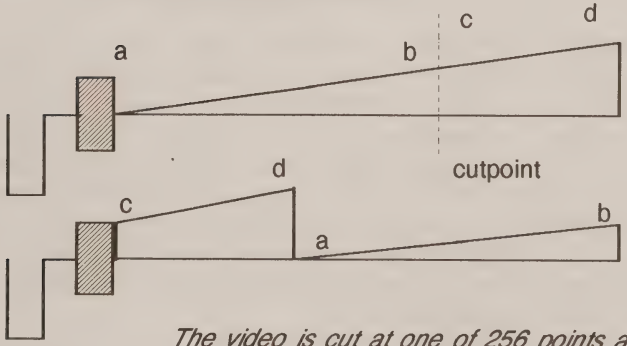
This digital video technique is the most secure. The digital data of the samples is encrypted using an algorithm such as the DES or RSA. It is presently used for the most secure applications such as high priced programming distribution.

Line Shuffle



The order of the lines is changed though the video information remains the same.

Line Cut And Rotate



The video is cut at one of 256 points and the segments are rotated about that point. There is an element of cloaking on the cutpoint. Descrambling involves delaying the /cd/ segment and clocking the /ab/ section out first.

Case Study: The RITC Discret 1 System

Video Scrambling: Video Line Delay.

The video information in each line is delayed by one of three delays; 0, 902 nS or 1804 nS. These delays are applied on a pseudo random basis so that the scrambled video takes on a ragged form.

Audio Scrambling: Spectrum Inversion.

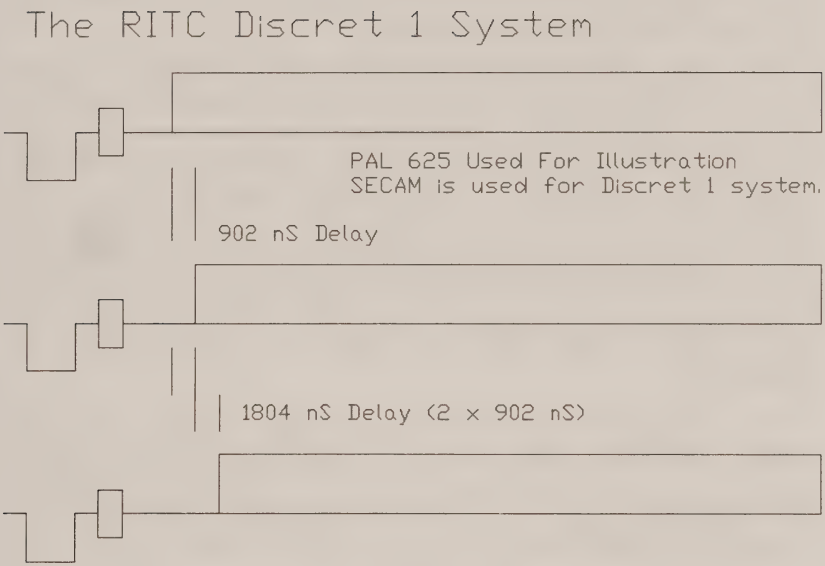
The audio is spectrum inverted around a 12.8 KHz carrier. This carrier frequency is derived from the system clock in the official descrambler.

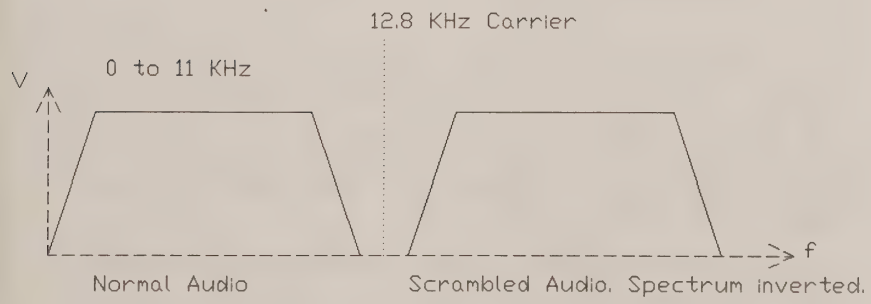
Users: Canal Plus France, the EBU and TV-5.

In November 1984, Canal Plus started transmission using the Discret 1 scrambling system. The system was unwisely proclaimed as being hackerproof. At first glance, there was good reason to believe in its security. The official descrambler used custom integrated circuits and was microprocessor controlled. Individual descrambler could be turned on or off by the headend. So what went wrong?

In the December 1984 issue of the French 'Radio Plans' magazine, there was an article on how to construct a pirate descrambler for Canal Plus. Naturally the people at Canal Plus were not pleased. They took legal action against the magazine and were successful. The magazine was seized by the court. It was decided that the 'Radio Plans' design did not infringe the patent but it was an incitation to theft. Enough photocopies of the article were circulated so that anybody who wanted them could get them. The problem was compounded by the fact that a Paris newspaper published the article. Things are now very different in France. Piracy is a serious offence.

The Discret system existed before Canal Plus decided to use it. It was primarily used for the TV5 links to Tunisia. When it was being used for that application, there was very little piracy because there were very few pirates with the necessary satellite reception equipment. The Canal Plus situation involved the use of terrestrial transmitters and as such the signal was widely available.


The RITC Discret 1 System
PAL 625 Used For Illustration
SECAM is used for Discret 1 system.
902 nS Delay
1804 nS Delay (2 x 902 nS)


12.8 KHz Carrier
V
0 to 11 KHz
f
Normal Audio
Scrambled Audio. Spectrum inverted.

The Discret system is a dual facility system. It scrambles the video and the audio. Most of the systems before Discret affected the synch pulses and sometimes the audio. The Discret system actually processed the video. It is primarily a baseband scrambling system. The RF signal has to be demodulated and turned into composite video and audio before it can be descrambled.

The advent of the SCART or Peritel socket ensured that the hookup of the descramblers would be efficient. Under French law all colour televisions had to have a SCART socket. Two types were manufactured; an RF type and a baseband type. The RF type had its own tuner and remodulator. It was primarily intended for use with televisions that predated SCART sockets. The baseband descrambler would connect directly to the SCART connector on the television. The television's tuner/demodulator circuit would provide the descrambler with composite video and audio. The descrambler would descramble the signals and return the clear video and audio signals to the television.

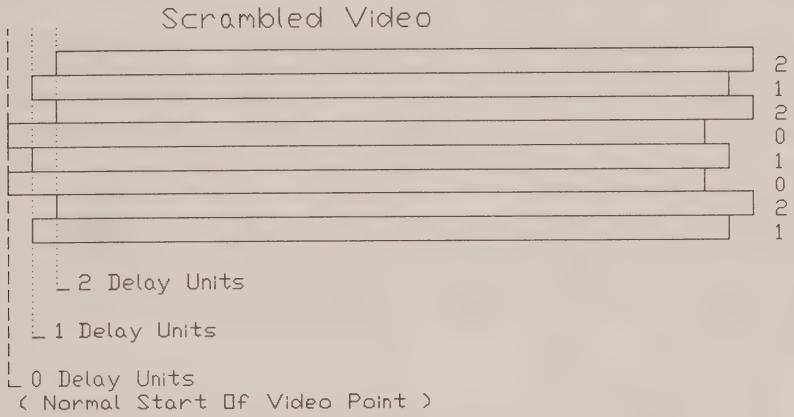
The video scrambling on the Discret system is known as "line delay". The active video section of each line is pseudo-randomly delayed by one of three delays; 0 nS, 902 nS or 1804 nS. This type of scrambling gives the video a very ragged look on the screen. The entertainment value of the picture is not totally destroyed.

The audio scrambling used is called "Spectrum Inversion". The audio spectrum is rotated about a carrier frequency. This makes the audio sound like Donald Duck on LSD. The lack of audio on the scrambled Discret signal destroys the entertainment value.

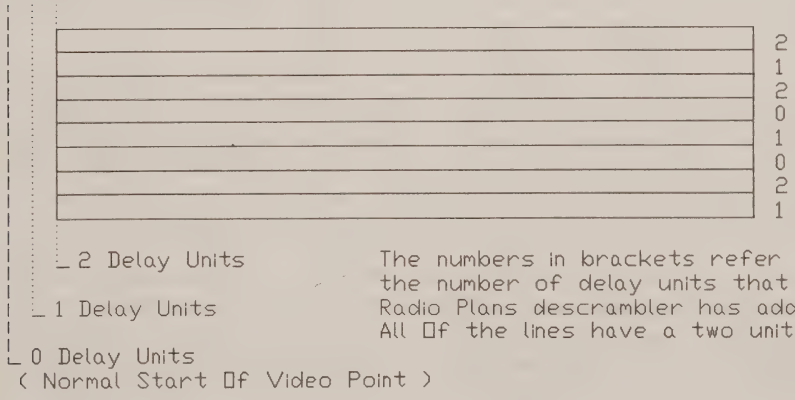
The sequence of delays is not random but pseudo-random. It repeats after six fields. The official descrambler required the customer to type in a pass number. For the first month, any number would work. After that, the customer's own pass number would only work on his own descrambler. The 'Radio Plans' design did away with all of that complexity. Of course the simplicity of the 'Radio Plans' circuit made it easy to for Canal Plus to counter.

The rise from black level to the start of active video was detected. A time slot or window circuit was used to check where the active video started. Three slots were used. If the active video started in the first slot, then the video was not delayed. If it started in the second slot, the video was delayed by 902 nS. If the video started in the third slot, then the video was delayed by 1804 nS.

RP Video Descrambler Operation



Video As Descrambled By The RP Descrambler



The numbers in brackets refer to the number of delay units that the Radio Plans descrambler has added. All Of the lines have a two unit delo

The 'Radio Plans' design ensured that all of the lines of video had 1804 nS delay. This was, in principle, a simple operation. If the video was not delayed, then it was passed through an 1804 nS delay. If the video was delayed by 902 nS, then the video was passed through a 902 nS delay. If the video was delayed by 1804 nS, then it was passed without introducing any delay.

The main problem of descrambling the signal lay in delaying the video. A simple solution was found. A colour transient improver IC, the TDA4560, was used. This IC had a gyrator delay line that could provide an 888 nS delay. Two of these ICs were used in the design. The IC naturally became difficult to obtain. Glass delay lines and even LC delay lines were tried.

The method of operation of the 'Radio Plans' design made it easy to defeat. Canal Plus injected a level other than black into the delay area. This fooled the start of video detector circuit into thinking that the video was not delayed. As the expertise of Canal Plus grew so did that of the hackers.

The fixed level modification to the system was easily overcome by the hackers. Since the level of the signal injected into the delay area was constant, a comparator circuit was used to detect it. An EXOR logic gate was then used to check if it was a flat level such as black, grey or white. Of course the addition of a noise burst instead of a level fooled the comparator circuitry.

Some hackers departed from the 'Radio Plans' design and developed microprocessor based descramblers. These descramblers detected the start and end of the six field sequence. When the sequence changed each month, the microprocessor would "learn" the new sequence. This is the format that many of the pirate descramblers now use. Even these descramblers now have a limited lifespan.

When Canal J introduced an upgrade, the microprocessor based pirate descramblers were affected. The following explanation is a simplified one. This was due to "false flags" and an extended sequence. The end of a sequence is clearly flagged in a Discret signal. The descramblers used this to lock or initialise their "learn" routines.

Under ordinary circumstances, the sequence was six fields in length. A sequence flag should therefore appear every six fields. A false flag is where the end of sequence flag appears when it shouldn't. This caused the pirate descrambler to initialise when there was no need to. The sequence length was also changed.

Hacker Descrambler Operation

The video signal is passed through three buffer amplifiers, two delay lines and a multiplexer. A smattering of logic circuitry is used to preserve the synch signals and the color burst. The video signal is also fed to the start of video detector. This circuit detects the rise from black level at the start of the video information. The output of this circuit is fed to a logic circuit called the delay detector. By using a series of monostables triggered by the line synch pulse, the delay is checked by determining the period in which the video starts. The period of each monostable is 902 nS. The output from this circuit controls the multiplexer. If the signal has zero delay, then it is fed through the two delay lines. If the signal has a one unit delay, (902 nS), then it is fed through one delay line. If the signal has two unit delay then it is fed straight to the multiplexer. The descrambler ensures that all the lines have a two unit delay. This produces a black line at the left hand margin of each frame, though it is generally lost in the overscan with most televisions.

The 'Radio Plans' descrambler has an inherent weakness in that it relies on the detection of the rise from black level to start of video in each line. If the delay was filled with a level other than black, then the 'Radio Plans' descrambler would not work. This is precisely what Canal Plus did in an early ECM.

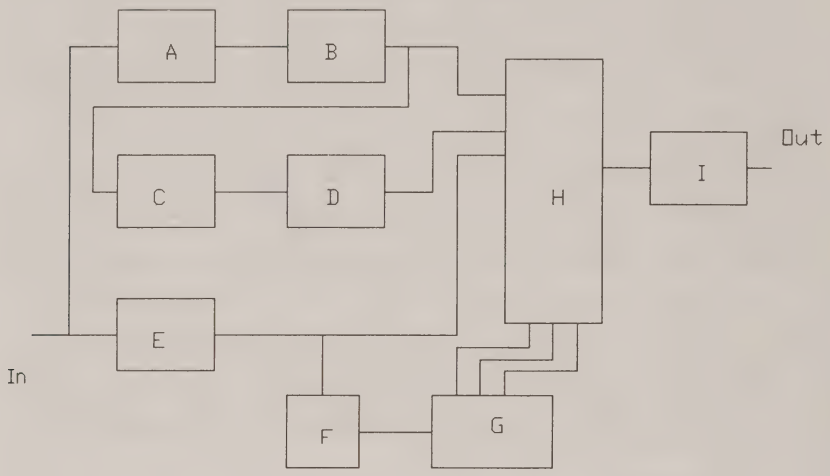
Other Information

There is a PAL version of the system in operation by the RAI via the ECS satellites. This version of the Discret system, known as Discret 12, uses smaller delays.

The Discret 12 system is a digital based system. The video has to be digitised in order to scramble and unscramble it. The delays are introduced into the digitised video using digital shift registers.

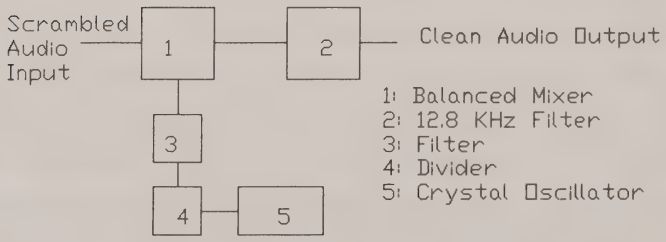
The hacker design for this system digitises the signal in much the same way as the official descrambler. The pre start of video section of each line is sampled a number of times. The width of each sample corresponds to the smallest delay time. If the byte does not correspond to the converted equivalent for black level, usually 00000000 binary, the video has started. This is checked using an eight input NAND gate. There are two ways in which the descrambler can clock out the digitised video. The existing line can be delayed to match

Radio Plans Video Descrambler



A: Delay Line 1
B: Black Level Clamp / Amplifier 1
C: Delay Line 2
D: Black Level Clamp / Amplifier 2
E: Black Level Clamp / Amplifier 3
F: Start Of Video Detector
G: Delay Selector
H: Multiplexer
I: Output Amplifier

Radio Plans Audio Descrambler



1: Balanced Mixer
2: 12.8 KHz Filter
3: Filter
4: Divider
5: Crystal Oscillator

up with the most delayed line as in the Discret 1 descrambler or the video can be delayed until what would be the next line period and then clocked out and converted to analogue at the correct time.

The Discret system is inherently insecure and most of the upgrades have been hacked within a very short time. The most common upgrade is to change the sequence of the delays and fill the delays with non-black levels. The main problem that the system faces is that the pirate descramblers are "clever". The microcontrollers in the pirate descramblers actually learn each new sequence.

In Ireland, Cablelink actually used this system for a while. They did not like it and found it unreliable. The descramblers that they were supplied with appeared to be models converted from the original French types.

There are rumours that a few of the MMDS franchises in Ireland are considering adopting Discret. The rationale being that there is a strong legal framework to protect them. This over reliance on legal safeguards is both stupid and dangerous. While the system might initially protect the franchise from hacking, it is a liability when considered in a long term light.

The Discret system is too old to be a viable system on anything other than low pay services. It is not secure enough to protect premium channels and hacker versions of the decoders are easily purchased.

The most dangerous aspect of the Discret decoder is that the critical addressing data is held in an EEPROM that can easily be read. In this respects it carries a flaw that was common in systems designed in the early eighties.Once the contents of the EEPROM can be copied, it is possible to create a set of cloned decoders merely be reprogramming the other official decoders with the same data. Naturally the programme provider could find out about the clone master and knock the clone network out.

Case Study: The OAK Orion System

Video Scrambling: Horizontal and vertical synch replacement, random or sequential field or line inversion.

The usual horizontal and vertical synch pulses are removed from the scrambled video and replaced with 2.5 MHz bursts. The video on each line can be inverted or normal polarity. A pulse situated just before the start of video in each line indicates the polarity of the video. The inversion can take place on a line, field or frame basis.

Audio Scrambling: Digital audio with encryption facilities.

The audio is digitised and compressed. The digital audio samples are then inserted into what would normally be the horizontal blanking interval.

Users: Sky Channel. (1982-1987)

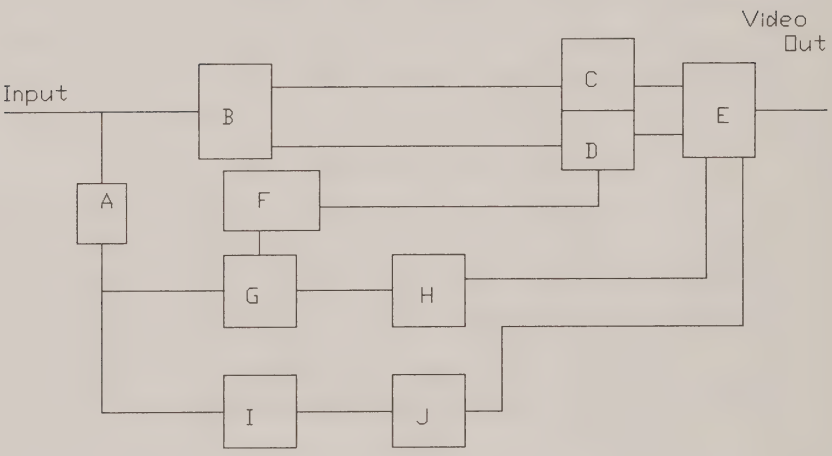
The Orion of Oak-Orion stands for Oak Restricted Information and Operation Network. The Oak-Orion scrambling system is a lot more secure than most hackers seem to think. In Europe, SKY has been the only satellite service to use this system. The minimum security level has been used for this application as SKY was not really a PAY-TV station in the true sense. The audio facility on the waveform was not used on SKY as monophonic and stereo subcarriers were transmitted with the signal.

Six possible inversion modes can be used in the system. One of four video inversion modes can be used during each field; inversion on odd lines, inversion on even lines, all inverted or no inversion. The control sequence for this option is to be found in line twenty-two. The Oak-Orion system is patented and the original patent application, (No: US 4353088), also includes two further options. The voltage level of the digital packet in each line could be shifted or alternatively it could be varied by a sinewave gated to vary the levels in the horizontal blanking period.

Variants of the system are still in use. It is however being replaced by more secure systems. As it dated from the early eighties, the system was remarkable for the amount of security it offered. It was let down by the fact it could be hook hacked.

The OAK ORION System
PAL 625
1V0
0V7
Polarity Key - High = Inverse Video
Colour Burst
3 Bytes PCM Digital Audio
2.5 MHz Synch Burst

Typical Hacker Descrambler Block Diagram



A: 2.5 MHz Detector
B: Differential Video Amplifier
C: Normal Video Switch
D: Inverse Video Switch
E: Synch Insertion Circuit
F: Polarity Pulse Detector
G: Line Separator
H: Line Monostable
I: Frame Separator
J: Frame Monostable

US Hacker Design For ORION Descrambler.

A: 2.5 MHz PLL
B: Differential Video Amp
C: Normal Video Switch
D: Inverse Video Switch
E: Synch Insertion Circuit
F: Polarity Bit Sampler / Control
G: Divider To Line Pulse
H: Divide To Field Pulse

Hacker Descrambler Operation:

The simplest hacker descramblers detect the 2.5 MHz synch bursts and use a number of monostables to recreate the line and frame synch signals.

The average hacker descrambler consists of the following blocks; an inverting video amplifier, a 2.5 MHz synch burst detector, schmitt trigger inverters, line synch monostables, an integrator, a frame synch monostable and a synch re-insertion circuit. A number of circuits can be used for the 2.5 MHz synch burst detection. These can vary from a diode detector to a video demodulator IC operating at 2.5 MHz. The synch re-insertion circuit can either be a CMOS switch type or a transistorised type.

Every line has an inversion bit preceding the video information. If the inversion facilities were ever to be used, then the hacker decoder would have to sample this bit and use a multiplexer prior to the synch re-insertion circuit to switch between positive and negative polarity video.

A descrambler for this system is covered in the Pink And Brown Book. It is a very elaborate method of descrambling the signal. A generic descrambler or synch generator Unfortunately this system is no longer in use on satellite links in Europe. It would have been easy for Sky to have defeated the hackers by introducing another level to the systems as the hacker descramblers that were used were crude and simple in design.

There is no information in Europe to suggest that the digital audio was hacked. The primary reason for this non-event was the availability of an unscrambled audio subcarrier. The situation was somewhat different in the USA. It was possible to buy an EPROM which, when inserted in place of the system ROM, gave access to every channel using ORION.

Case Study: The LuxCrypt System

Video Scrambling: Horizontal and vertical synch replacement, random or sequential field or line inversion.

The usual horizontal and vertical synch pulses are removed from the video and replaced with 5.72 MHz bursts. The video on each line can be inverted or normal polarity. The inversion can take place on a line, field or frame basis.

Audio Scrambling: Digital audio with encryption facilities.

The audio is digitised and compressed. The digital audio samples are then inserted into what would normally be the horizontal blanking interval. Only two bytes of the three byte data burst are used for digital audio. The other byte is used for synch information and perhaps line polarity information. This digital audio facility is not used in the LuxCrypt implementation.

Users: RTL4-Veronique

This system is in some ways similar to the forerunner of the ORION system. The primary difference between the LuxCrypt as used on RTL-4V is the lack of the 2.5 MHz synch burst. This means that a pirate ORION descrambler will not work on this system without modification.

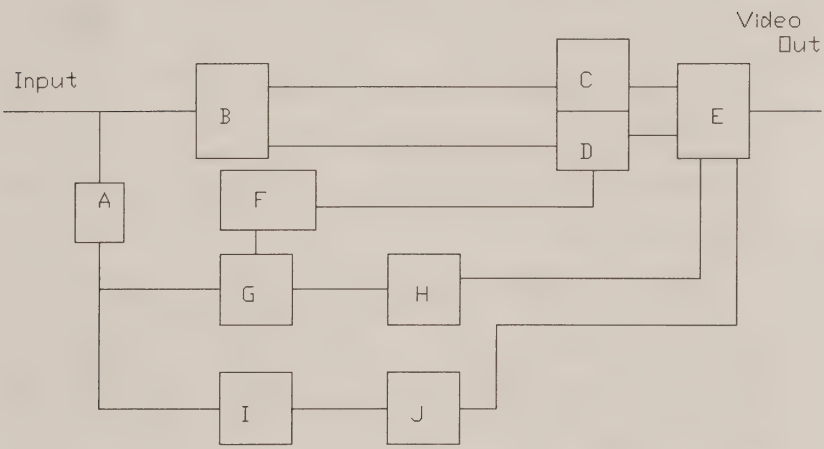
The primary reason for the use of this system by RTL4-V is copyright. RTL4-V does not have European copyright for some of the programmes shown on the channel.

The video inversion can be based on the amount of white or black in the scene. This type of inversion is known as average peak level or APL, pronounced “apple”. These inversions take place on a three second basis.

The APL inversion was introduced in January 1990. The effect on the pirates was significant. Many of the commercial pirates had completed their designs and were oblivious to the fact that the APL inversion facility existed. Many were getting ready to ship their completed descramblers to waiting customers when RTL-V struck with the upgrade. This turn of events added at least another month to delivery dates.

The LuxCrypt System
PAL 625
1V0
0V7
Polarity Key
Colour Burst
Digital Audio-PCM

Typical Hacker Descrambler Block Diagram



A: 4.0 MHz Data Detector
B: Differential Video Amplifier
C: Normal Video Switch
D: Inverse Video Switch
E: Synch Insertion Circuit
F: Polarity Detector
G: Line Separator
H: Line Monostable
I: Frame Separator
J: Frame Monostable

RTL4-V uses polarity inversion on a random basis. To date this has only been on a field basis rather than a line basis. The aim is to upset the old dual FilmNet RTL4-V descramblers. Most of the RTL4-V pirate descramblers are not affected as they are actual clones of the official model.

Hacker Descrambler Operation:

The simplest hacker descramblers detect the 4.0 MHz synch bursts and use a number of monostables to recreate the line and frame synch signals. Other versions detect the color burst in each line and count the number of color bursts to trigger the field pulses.

The average hacker descrambler consists of the following blocks; a video amplifier, a 4.0 MHz synch burst detector, schmitt trigger inverters, line synch monostables, an integrator, a frame synch monostable and a synch re-insertion circuit. A number of circuits can be used for the 4.0 MHz synch burst detection. These can vary from a diode detector to a video demodulator IC operating at 4.0 MHz. The synch re-insertion circuit can either be a CMOS switch type or a transistorised type.

To hack the inversion facilities the hacker decoder would have to sample the white level - black level line in the Vertical Interval Test Signals. The condition of this line would indicate the polarity of the field. The polarity sample is then used to control a multiplexer which switches between positive and negative polarity video prior to the synch re-insertion circuit.

This can be defeated by the use of a byte of the digital information to control a line based inversion. This is possible though it is unknown if this option will be used on the RTL-Veronique implementation.

Apparently this system has been adopted by RTL5 though this implementation uses APL. As a result some of the old pirate designs do not work. However the XV2000 design has been reported working.

Case Study: Sound In Synch - EBU Format

Video Scrambling: Digital Sound In H. Synch

The video in the EBU sound in synchs system is not actually scrambled. Because the digital audio is inserted into the horizontal blanking interval, the synch stripper in the television can be confused. The picture appears ragged and at times can lose line stability.

Audio Scrambling: PCM With Crypto

The audio in this system is digitised and encrypted. In some cases the audio is unencrypted but a digital demodulator is required.

Users: European Broadcasting Union

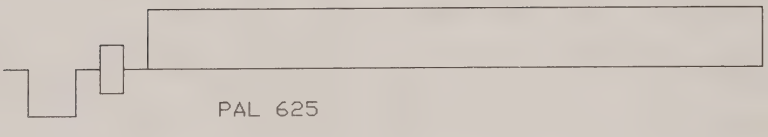
The EBU format system is designed to optimise the satellite power. On a normal satellite transmission, the audio is transmitted on a subcarrier in the range 5 MHz to 8 MHz. This consumes some of the available power. The EBU system economises by putting the audio in the video waveform. This means that the EBU transmission format is essentially only a video waveform. As a result, the power that would have been used for an audio subcarrier can now be used for the video. This gives a better CNR.

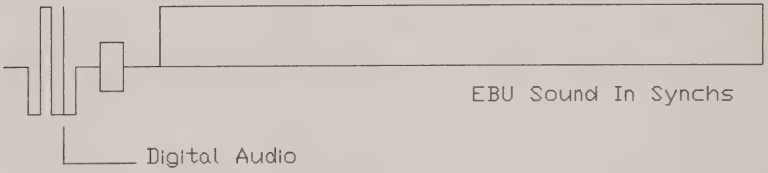
There are rumours that the ENU are considering a switch to either NagraKudelski Syster or VideoCrypt. The aim of this is to stop the piracy of the signals.

Hacker Descrambler Operation:

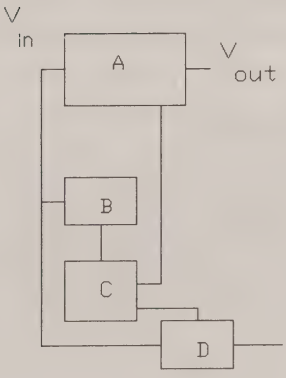
There is not a great demand for a hacker descramblers for this system. Most hackers would not waste time on the audio encryption without having a waiting market. The video on the other hand is easily hacked. It merely involves replacing the horizontal synch pulse area in the scrambled signal with a new properly timed horizontal synch pulse.

EBU Sound In Synchs





Typical Hacker Descrambler Block Diagram



A... Synch Re-insertion

B... Falling Edge Detector

C... Line Synch Monostable

D... Digital Audio Gate (EBU Only)

Case Study: Standard Electric Lorentz PCM2

Video Scrambling: Shortened H. Synch Pulse

The video in the SEL system is not actually scrambled. The horizontal synch pulse is shortened from 4.7 uS to approximately 1 uS. This causes the television synch circuitry to lose line lock. The frame pulses are untouched and as a result, the picture may lock vertically but it will not have total horizontal lock.

Audio Scrambling: Digital Audio.

One audio packet is placed after the shortened horizontal synch pulse. The other audio packet is placed after the color burst.

Users: SAT-1

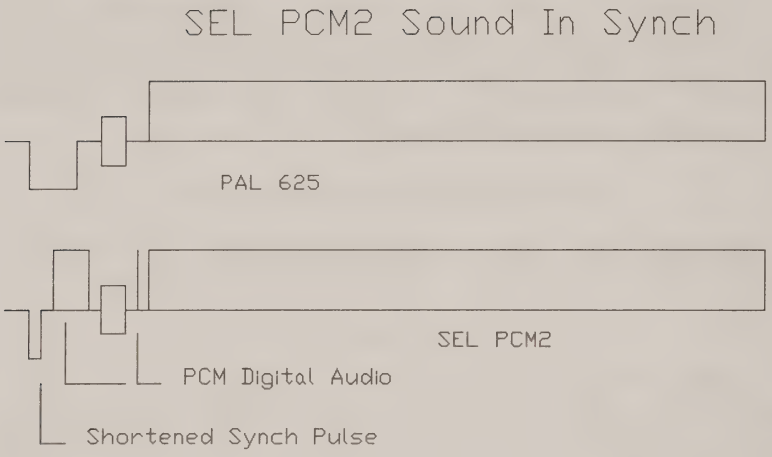
The SEL PCM2 system has two main differences from the EBU system. The digital audio is placed in the line blanking interval at two points; one packet before the color burst and one packet after the color burst. When the system was in use in Europe, the second packet was rarely used. The second difference was the use of a shortened line synch pulse. This pulse was shortened to approximately one microsecond.

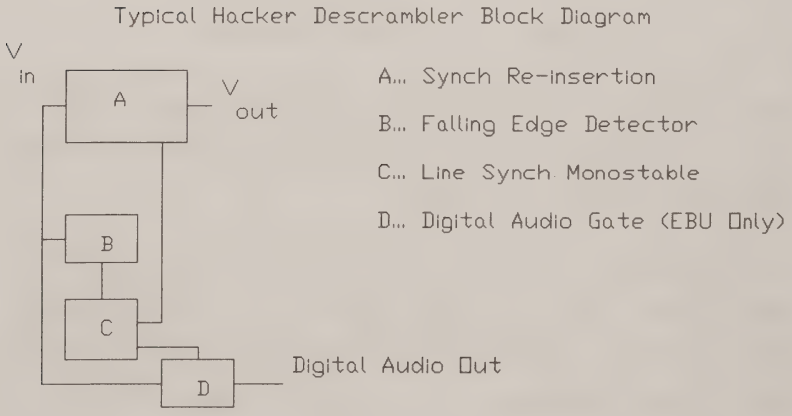
Hacker Descrambler Operation:

The video section of the SEL PCM2 is relatively easy to descramble. The hacker descrambler uses the shortened horizontal synch pulse to trigger a properly dimensioned horizontal synch pulse. This new synch pulse is then inserted into the scrambled waveform in place of the shortened synch pulse.

A standard synch stripper can be used. The stripped synch is fed to a monostable set to give a 4.7 uS pulse. The 1 uS synch pulse is also used to trigger a set of gating monostables to gate the digital audio to the demodulator. The digital audio levels are between black level and white level. This implies that the signal should be well clamped prior to descrambling. Sometimes if the clamp is badly designed, the shortened synch pulses can be damaged.

At the present, the SEL PCM2 system is not being used in European satellite broadcasting. According to available information, the audio was not hacked.


SEL PCM2 Sound In Synch
PAL 625
SEL PCM2
PCM Digital Audio
Shortened Synch Pulse


Typical Hacker Descrambler Block Diagram
V in
A
V out
B
C
D
Digital Audio Out
A... Synch Re-insertion
B... Falling Edge Detector
C... Line Synch Monostable
D... Digital Audio Gate (EBU Only)

Case Study: The FilmNet System - SATPAC

Video Scrambling: Synch Shifting. Sequential Field Video Inversion

Audio Scrambling: Modified NICAM With Crypto

Users: Defunct

The Filmnet / SATPAC / Matsushita system was first used on Filmnet on 01/Sept/1986. Up to that point in time, the channel was one of the most popular film channels. The Filmnet system is perhaps one of the systems with a Pan-European attraction for hackers. Its main product is American originated films. These films are left in their original Amglish, (American English). There is a powerful teletext based multilingual subtitling facility available so that the viewer can select the subtitling in a number of languages. This coupled with the low cost of a pirate descrambler has fueled the demand for descramblers.

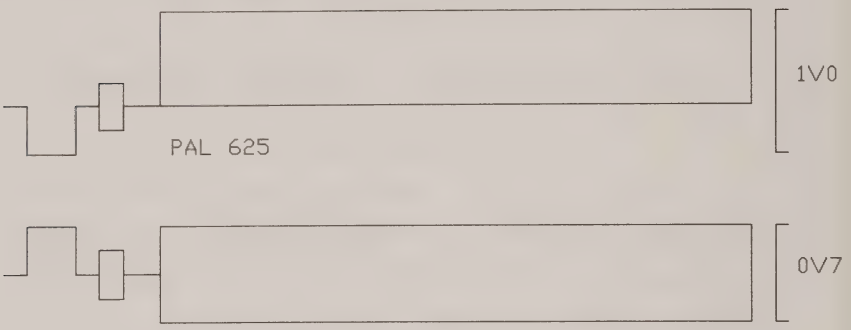
The FilmNet channel has copyright for the films in a few countries in Europe. this means that it cannot supply descramblers to viewers outside these areas. This created a demand for pirate descramblers which was satisfied by pirate descrambler manufacturers. Another factor in the popularity of Filmnet in the UK is the pornographic movies shown on Wednesday and Saturdays.

The FilmNet SATPAC system is an old system. It was developed in the early eighties and reflects the available technology of the time. It interferes with the polarity of the video and the level of the horizontal blanking intervals. This means that it is not permitted on some of the cablenets of the more technologically advanced European countries.

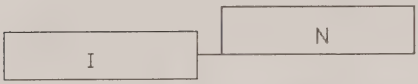
Filmnet is one of the most advanced channels in Europe in one respect - subtitling. Using the teletext facility, the viewer can select the subtitling language from a number of European languages. This is similar to the closed captioning facility in the United States.

The first level of Filmnet was employed from 01/Sept/1986 to 23/March/1987. The first phase was extremely simple to hack and there was a booming market in pirate or blackbox descramblers. The upgrade that occurred on 23/March/1987 dented the market. It was an easy hack. The video in each alternate field was inverted. The effect on the pirate market was devastating. The upgrade went into

The FilmNet/Matsushita System



Level 1 Suppressed Synch / Inverted



Level 2 - Alternate Field Invert
Two Field Sequence

Level 3 - Four Field Sequence, Fourth Field Normal

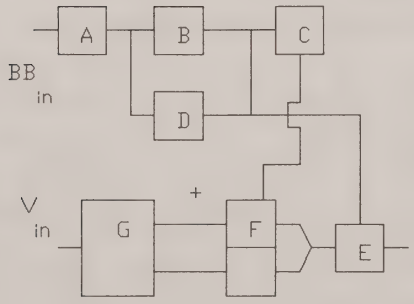
Typical Hacker Descrambler Block Diagram

A... 7.56 MHz Demodulator

B... Integrator (Frame)

C... Flip Flop

D... Line Locker
E... Synch Inserter
F... Multiplexer



operation a few days before one of the largest European satellite shows, Cable And Satellite 1987. This rendered many of the demonstration models useless.

The Filmnet system was upgraded over Christmas 1989. The upgrade took place over a few days. The system was fully updated by 24/12/89. It was the worst possible Christmas present for pirate descrambler owners and manufacturers. Many of the pirates were working over the holiday period in order to get their stock upgraded. The impact of the upgrade was considerably less than that of March 1987. Many of the pirate descramblers were not eliminated. Those that were affected were quickly upgraded and the estimated effective lifetime of the upgrade is two weeks. Most pirates took advantage of the holiday period and as such had working descramblers ready for January 1990.

At the end of January 1990, FilmNet switched back to the two field sequence with rather nasty effects for some pirate descrambler manufacturers. They had hardwired the descrambler upgrades for the four field sequence. The descramblers did not work after the downgrade. This produced a lot of angry customers who wanted their money back. Some of the more recent pirate descrambler manufacturers were bankrupted as a result.

When FilmNet introduced their digital audio in 1991, it effectively nuked the market. It did not have the effect that FilmNet had hoped for. Instead of killing off every pirate manufacturer it only killed off the smaller firms. The larger firms concentrated on hacking the digital audio. Hi Tech actually had the FilmNet digital audio ASIC reverse engineered and after examining it created a new one. The Hi-Tech ASIC and decoder actually outperformed the official FilmNet digital audio decoder. The digital audio is covered in Chapter 4.

Hacker Descrambler Operation:

There are a number of methods used by the hackers to descramble the FilmNet signal. The commonest are; synch recombination using triggered monostables, synch recombination using a PLL and synch regeneration. We will only use the triggered monostable design as an example.

The first level that FilmNet used was an inverted line and suppressed horizontal blanking interval.

The composite synch signal for the Filmnet system is transmitted on a carrier at 7.56 MHz. This carrier is demodulated using a standard demodulator.

This composite synch signal is then split into frame synch, (using an integrator), and line synch. The first two line monostables phase the line synch with the synch position in the scrambled video.

A noise gate is used to the detect the horizontal synch interval in the scrambled video. The output of the noise gate is ANDed with the phased line synch. This gives a correctly timed trigger line synch pulse.

The trigger pulse is fed to two monostables. These first monostable delays the pulse by 52 uS. The delayed pulse is then used to trigger the second monostable. This monostable generates a pulse the approximate width of the horizontal blanking interval. This pulse is used to pull down or shift the horizontal blanking interval in the scrambled video back to the unscrambled level.

Upgrade 1 - 23/03/1987

The video is inverted in each alternate field. The design uses a multiplexer to switch between the inverted video and normal video outputs of a differential output amplifier. The frame pulse is divided by two using a flip flop. This means that the output of the flip flop changes polarity once every field.

The actual flip from normal to inverse video does not take place at the exact end of one field. This means that the frame pulse must be slightly delayed by a monostable before feeding it to trigger the flip flop.

Upgrade 2 - 24/12/1989

The upgrade was not difficult to overcome. It was based on a four field sequence. The fourth field was normal polarity and the other three fields were inverse polarity. The pattern could be produced using two flip flops and an AND gate. The first flip flop divides the field frequency by two to give a 25 Hz square wave. The second flip flop divides the 25 Hz square wave by two to produce a 12.5 Hz square wave. The 25 Hz square wave and the 12.5 Hz square wave are ANDed. This produces a signal that goes high on every fourth field. A NAND gate can also be used.

FilmNet returned to the two field sequence in late January 1990. The aim was to cause maximum confusion among the pirates.

Upgrade 3: 5/11/1990:

FilmNet inserted a low level high frequency sine wave burst into the horizontal synch pulse tip. The frequency of the sine wave was approximately that of the colour subcarrier. This had two consequences. It upset descramblers that used the colour burst to lock on. They saw two properly timed, (relative to one another), colour bursts. It also affected descramblers that determined the video polarity by comparing the level of the synch tip with the horizontal blanking level.

This upgrade had the most widespread effect in the Blackbox industry. It was expected by some of the veteran manufacturers but some of their descramblers were mildly affected. It was generally a case of adding one or two components to the board as they had designed their descrambler with this upgrade in mind. Some of the more recent additions to the industry were nearly obliterated by the upgrade - much to the amusement of the veteran pirates.

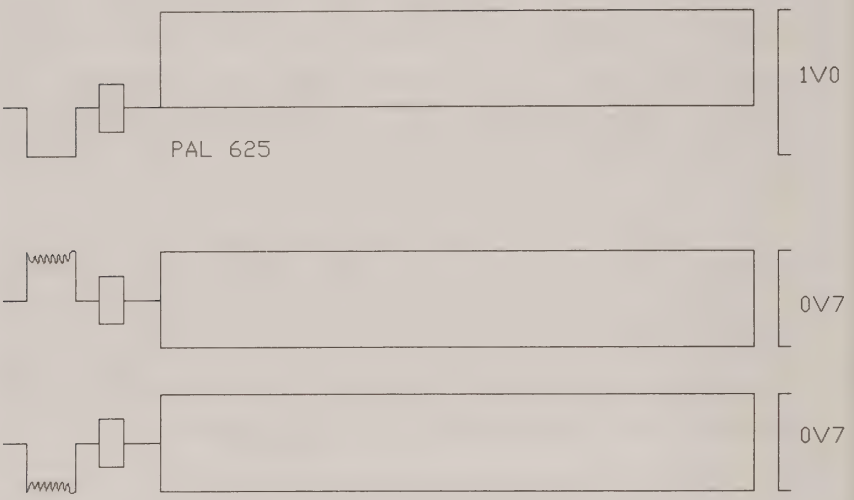
Upgrade 4: December 1990:

In December 1990, FilmNet started to vary the amplitude of the burst in the horizontal synch pulse by amplitude modulating the burst with a very low frequency, 1 Hz, wave. The logic behind this was clever. Most of the synch tip sampling descramblers had placed a very low value capacitor, typically 100pF into the comparator circuit to filter out the burst in the synch tip. The low frequency would remain after the 100pF capacitor had filtered out the burst. This varying level would cause problems for the comparator as it was forced to interpret a signal as being inverted when it was actually normal polarity. Most of the pirate descramblers were easily modified to cope with this upgrade.

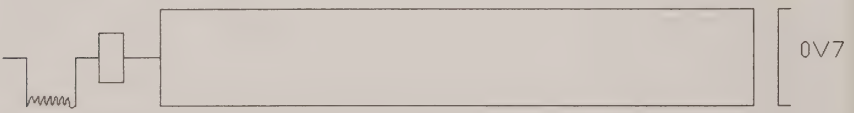
Upgrade 5: January 1991:

The first level of FilmNet's system is suppressed synch and no inversion. In January 1991 FilmNet switched off the inversion. This move surprisingly took out a few of the descramblers on the market. It did not affect the descrambling section of the descramblers but rather the autoswitching circuitry. Many of these descramblers used the inverted synch pulses in the FilmNet signal to trigger the descrambler

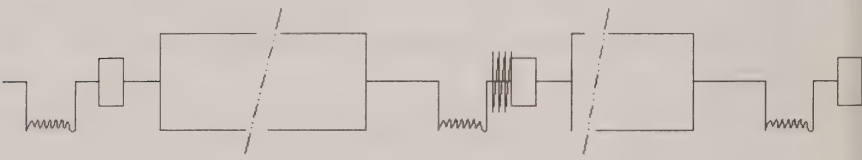
FilmNet Upgrades



November 1990 Upgrade. Burst In Synch Tip. Alternate Inversion still in use.



January 1991 Upgrade. Suppressed Synch And No Inversion



The upgrade of 25/03/1991 introduced a false colour burst into various lines. This gave a pseudo line delay effect on some colour burst locking descramblers.

into operation. Since there were no inverted synchs, the descrambler interpreted the signal as being clean. The descramblers affected by the modification were easily upgraded.

Upgrade 6: March 1991:

In March 1991, a sequence of colour bursts was placed in the vertical synch. These prolonged bursts confuse the burst counting circuitry in some of the colour burst locking descramblers. The result is that the descrambler doesn't know where to put the vertical synch. This results in the picture rolling on the screen. Many of the descramblers on the market could be tweaked by the user to overcome the problem.

Upgrade 7: March 1991

The double glitch modification was aimed at descramblers using the 7.56 MHz composite synch carrier. It inserted a second pulse adjacent to each pulse. This was intended to unlock PLLs. The modifications generally involved disabling the pulse detection after the end of the first pulse. This was achieved with a monstable and multiplexing circuit.

Upgrade 8: June 1991

Digital audio was introduced. This was the end of an era. The pirate descrambler market created by the launch of ASTRA disappeared over the last year. To date only Hi-Tech have hacked the digital audio.

Upgrade 9: September 1992

FilmNet ceased PAL transmissions via ASTRA. They continue to broadcast via ECS2-F1. The move has not actually affected the sales of Hi-Tech digital audio decoders. It is possible to fit a second LNB to many offset dishes. This allows the reception of ASTRA and ECS2-F1. As a result of running two channels in the one transponder, FilmNet reduced the power on the signal. This has caused a few problems on small dishes.

Footnote:

In December 1993 FilmNet ceased using the SATPAC system on their satellite feeds. Instead they replaced it with EuroCrypt-M. Unfortunately EuroCrypt-M is also hacked.

Case Study: Telease MAAST / Sat-Tel SAVE

Video Scrambling: Sine wave interference. Video inversion. Video amplitude reduction.

The video in the scrambled signal is reduced by 3dB, (6dB in Europe), inverted and has an interfering sine wave added. The frequency of the sine wave is approximately six times the horizontal raster frequency, (15625 Hz x 6= 93750 Hz).

Audio Scrambling: Spectrum Inversion.

The carrier is derived from the frequency of the interfering sine wave. The sine wave frequency is divided by six to generate the carrier.

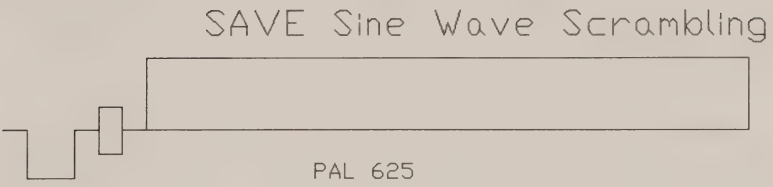
Users: Premiere [deceased], Canal 10 [deceased], Red Hot Dutch [deceased]

The MAAST system was developed by Telease of California. It was manufactured and marketed in Europe by Sat-Tel, a now defunct UK company. The system is essentially a low security type.

The system reduces the amplitude of the video signal, inverts it and adds a sine wave. The sine wave is close in frequency to the sixth harmonic of the line frequency. This ensures that any attempt to filter out the interfering sine wave and antiphase it with the scrambled video will leave a beat frequency patterning on the descrambled video. The reason for this is that the sixth harmonic of the line frequency is also pulled out by the filter.

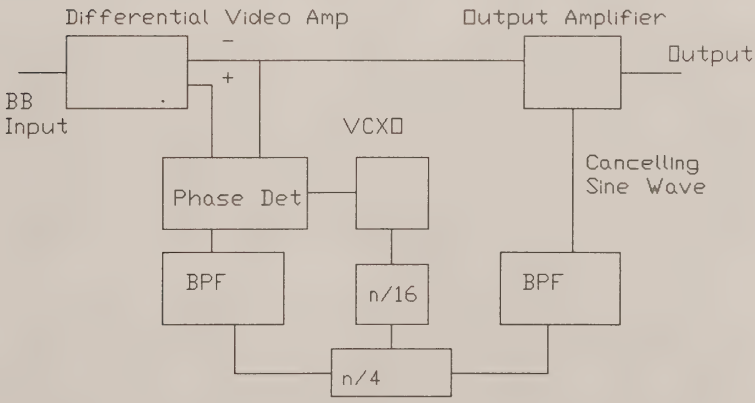
The level of video reduction differs. The US version reduces the video by 3 dB and the European version reduces the video by 6 dB. This difference is primarily related to the transponder bandwidth. The US version typically operates in a 36 MHz bandwidth and the European version in a 30 MHz bandwidth.

While the system has fallen into relative disuse in the US, it is widely used in Europe. The now defunct Premiere channel used it. The hybrid form of BBC transmitted on the Intelsat at 27.5 degrees West used a more advanced form before switching to D2-MAC EuroCrypt. It uses a combination of frequencies that can be selected at random. The



SAVE
The video is attenuated by 6 dB and a sine wave of approximately 94 KHz is added to the video waveform.

Cancelling Sine Wave (Antiphase)



Typical Hacker SAVE descrambler

system is not very secure in its present form and has unused facilities. Security cannot be completely compromised for the sake of some desk jockey economist.

Hacker Descrambler Operation:

The basic hacker descrambler uses a voltage controlled crystal oscillator running at 64 times the frequency of the interfering sine wave. It is essentially a phase locked loop circuit. The VCXO increases the cost of the actual descrambler. Various low cost alternatives have been employed. One of the best of the European hacker designs used a 6.0 MHz ceramic resonator.

The MAAST / SAVE system has an audio scrambling facility. This facility is used in the US version but has not seen widespread use in Europe due to the common use of stereo subcarriers. In the standard audio scrambling facility, the audio spectrum is rotated around a nominal 15 KHz carrier. The highest frequencies then become the lowest frequencies and vice versa. The carrier used for the rotation is generally one sixth the frequency of the interfering sine wave.

The BBC audio scrambling facility is more complex. It is based on Spectrum Shifting rather than inversion. As a result the descrambler is decidedly more complex. A possible circuit for a Spectrum Shift scrambler and descrambler was published in the October 1991 issue of Elektor Electronics.

The BBC form of the video scrambling uses a number of frequencies for the interfering sine wave. This allows the operator to switch between the frequencies. The switch generally occurs in the time when the transponder is not carrying video. Most of the pirate descramblers that were used for the original single frequency system required a complete upgrade. The commonest form was the introduction of a new crystal and a switch. The cheaper and more versatile use ceramic resonators

The most recent channel to use the system was Red Hot Dutch. They switched from the system in 1993 to KeyCrypt / Enigma. The crystal frequency used in their variant was that of the 8085 system clock. Since this frequency divides down to 96 KHz, it did not take advantage of the strength of the SAVE system. The 96 KHz sine wave was too far away from 93.750 KHz for serious amplitude beat frequencies. Therefore some people achieved watchable pictures by inverting the video.

Case Study: Payview III

Video Scrambling: Synch modification, pseudo line delay, video inversion.

The horizontal blanking interval is raised above peak white level. This confuses the television receiver automatic gain control and clamping circuitry. When the scrambled video is displayed on a television set, the picture appears dark. The horizontal synch pulse is dithered or rapidly shifted in time. This causes a pseudo line delay effect on the scrambled video. The line video can be inverted on a sequential or random basis.

Audio Scrambling: Digital, but not used over satellite.

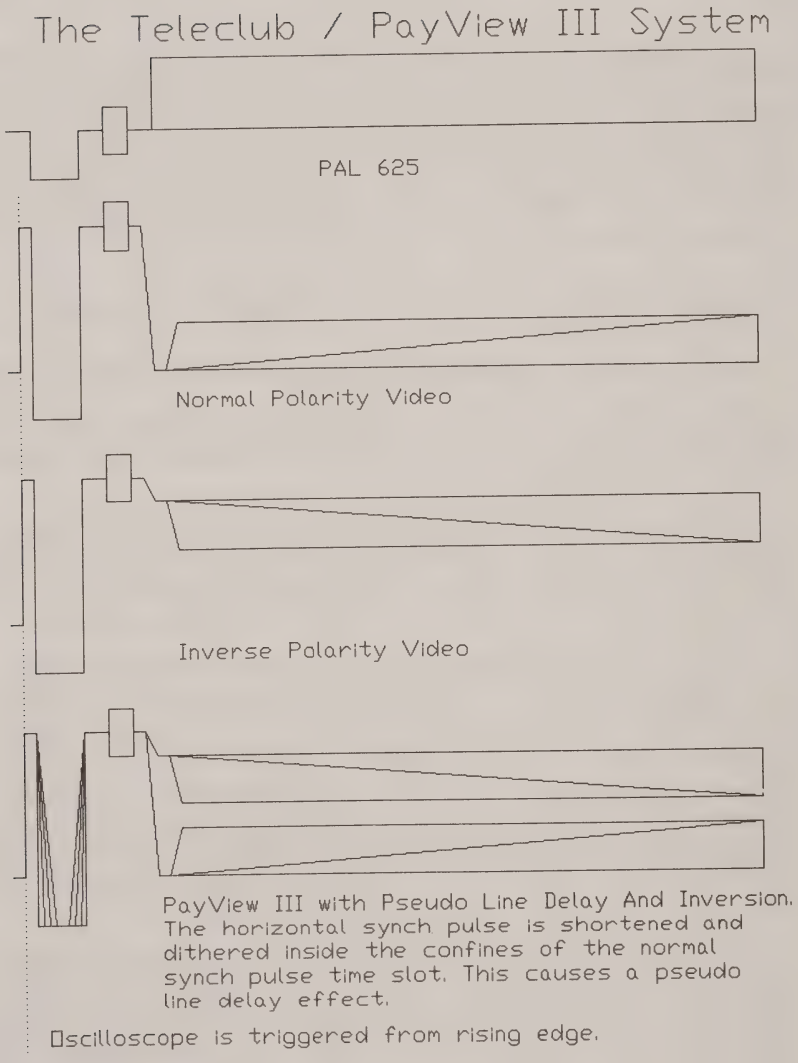
Users: Teleclub [Now using Syster] Canal 10 [Deceased]

The Payview III system was first tested via satellite for the now deceased Spanish Canal 10. This system was not eventually chosen for use on the channel.

Teleclub were testing this system sporadically throughout 1988 and introduced it in 1989. The system was employed in its basic form; alternate line inversion and no pseudo random line delay. This level was quickly hacked and pirate descramblers flooded the market.

The system is not difficult to hack in its basic forms but if random line inversion is used it will probably disable many of the pirate descramblers. The raised horizontal blanking section can cause problems with some types of satellite receivers. The main problem occurs with receivers with inadequate bandwidth. The Payview satellite transmission format used a 36 MHz transponder bandwidth. Some hackers tried to receive the signal using an poorly converted ASTRA bandwidth, (26 MHz), receiver. This causes a problem with the color burst which appears to be suppressed or attenuated.

When Teleclub introduced a rapid form of video inversion, many of the pirate descramblers were affected. In the majority of cases, it is simply a case of an out board modification. Unfortunately for some descrambler users, the manufacturers of the descramblers had ceased to exist.


The Teleclub / PayView III System
PAL 625
Normal Polarity Video
Inverse Polarity Video
PayView III with Pseudo Line Delay And Inversion.
The horizontal synch pulse is shortened and
dithered inside the confines of the normal
synch pulse time slot. This causes a pseudo
line delay effect.
Oscilloscope is triggered from rising edge.

Hacker Descrambler Operation

The original level of PayView was a very easy hack. The simplest descrambler relied on detecting the rise to above peak white. A comparator was used. The actual circuit is given as the Pseudo Line Delay Detector circuit in Chapter 3.

The rise to above peak white voltage was used to trigger a set of monostables. The monostables generated the properly timed synch and blanking level pulses. These pulses were used to gate a "pull down" down circuit and a synch reinserter. The "pull down" circuit restored the colour burst to its proper voltage level. The synch reinserter replaced the blanking and synch pulses.

The use of a synch reinserter was a necessary safeguard. Since many of the original pirate descramblers used the negative going transition of the horizontal synch pulse to lock on, they were nuked by the introduction of the pseudo line delay. Using the rise to above peak white as the lock point made that upgrade ineffective.

The video inversion also caused problems. Many of the earlier descramblers had field based sequence generators. They would have to be set with a DIP switch for the proper sequence. To counteract these descramblers, half sequences were used. As a result the sequence generators were knocked out.

Some of the better descramblers used the inversion key technique of detecting the video inversion. This method, was also locked to the rising edge, but the descrambler had a system clock operating at a multiple of the line frequency which generated the sample slot. The sample was taken at the start of the active video.

Eventually the only way to properly hack the system was to use a microcontroller based descrambler. These descramblers rapidly replaced the analogue versions. When Teleclub implemented an ECM, the only thing that needed to be upgraded in the descrambler was the microcontroller's EPROM.

Case Study: VideoCrypt

Video Scrambling: Line Cut And Rotate

Audio Scrambling: Spectrum Inversion - Not Used

Users: Sky, The Adult Channel, TV-Asia, JSTV

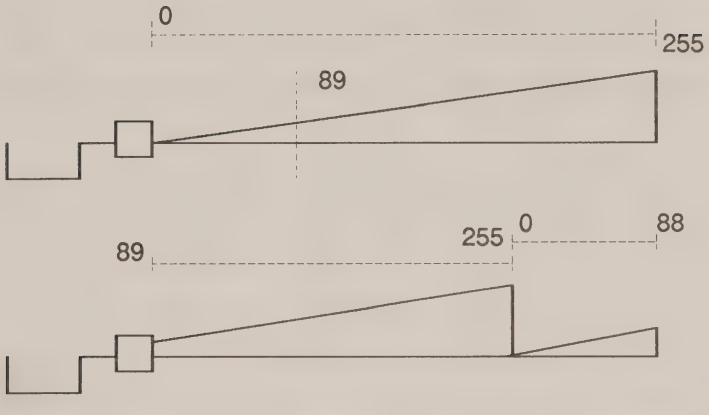
The VideoCrypt system scrambles the video only. It cuts each line of video at one of 256 possible cut points. It then rotates the video information around this cut point. There are 625 lines in the PAL system. Only 585 lines or so are used for video, the rest are used for non-video information such as test signals and teletext. This means that only 585 lines have to be scrambled.

The cut point on each line can be defined by one byte or eight bit word. The actual sequence of the cut points is pseudo random. The sequence is derived from a pseudo random number generator in the custom logic chip. This chip generates a sequence of numbers that will repeat if the sequence is left to run for long enough. The start point in the sequence is set by a seed transmitted over the air. This seed is changed every 2.5 seconds.

Sky Channel's publicity people announced that Sky was to use the most pirate proof system yet devised. This claim was made by the publicity people and as such it is treated with due cynicism by those in the signal security business. It should be noted that every system that was considered totally secure has been hacked. What would inspire such confidence, lack of brainpower ?

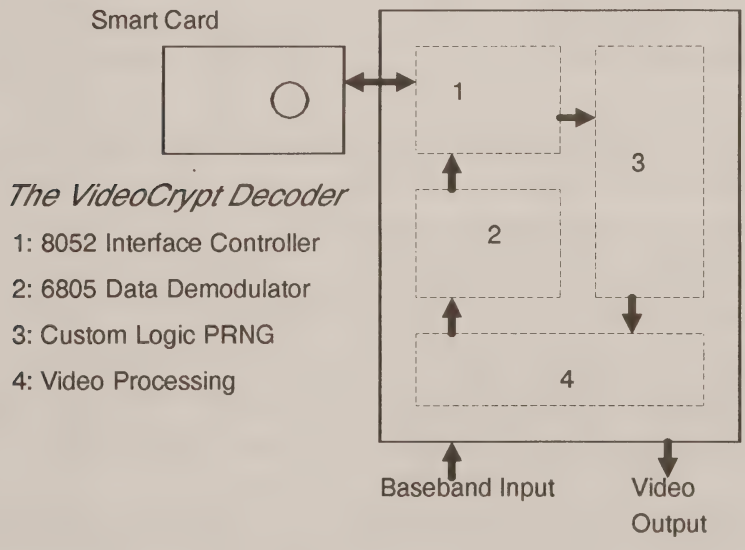
The encryption methods used to protect the keys and the over the air addressing data are some of the most advanced yet. Of course they have been compromised over the last year or so. The new card issue, 09 , has even suffered hacks less than two months after its introduction.

The decoder is controlled by a SMART card. The initial period for each card was to be three months. Due to the expense of distributing the cards, Sky tried to get as much time out of each card as they could.



VideoCrypt - Cut and Rotate Scrambling

The VideoCrypt system uses Cut and Rotate as its method of video scrambling. In the diagram above the cut points are clearly visible. In reality, these cut points are hidden or masked using various techniques. The Thomson patents may actually hold the clues to the exact nature of the scrambling and the transition masking.



The VideoCrypt Decoder

1: 8052 Interface Controller

2: 6805 Data Demodulator

3: Custom Logic PRNG

4: Video Processing

The SMART card differs from the Automatic Teller Machine cards in that it has built in circuitry. The ATM card stores the data on a magnetic strip on its back. This built in circuitry in the smart card holds the keys for decrypting the seeds and other data transmitted over the air.

The VideoCrypt system was developed jointly by the French Thomson company and News Datacom. The system is one of the more modern scrambling systems that makes use of digital television technology. The primary weakness of most of the non-digital scrambling systems on the market is that they affect the synch pulses in the video. This makes the signal unrecordable in its scrambled state. The VideoCrypt signal can be recorded in its scrambled state and then recovered. This factor has allowed yet another hack on the system - DDT. (see chapter 7 for full details of hacks on this system)

The critics of VideoCrypt have called it a halfway technology. In a sense it is. The D-MAC video scrambling system uses a double cut and rotate. It cuts and rotates the chrominance and the luminance separately. This would imply that the D-MAC video scrambling system is twice as secure as the VideoCrypt system.

The technical media in Europe have carried articles examining the security of the VideoCrypt system. There were some articles about the system in some low level magazines that were little more than regurgitated publicity data. The few articles that appeared in the technical media were by the top European authorities on satellite signal security. (OK - I wrote the articles) They were of the conclusion that the VideoCrypt system could be hacked - a conclusion that has been repeatedly justified over the last few years.

When I wrote the articles, more than a few of people disagreed with me. One journalist in particular wrote of VideoCrypt in such glowing terms that people began to think that he was employed by Sky. Of course he believed that VideoCrypt was invincible and it came as a nasty shock when it was hacked. The McCormac Hack, proposed in Version 2 worked. The write voltage limiting hack, as vaguely outlined on page 6-24 of Version 2 worked. The KENtucky Fried Chip hack worked. The Ho Lee Fook hack and DDT worked. Not exactly the most pirate proof system yet devised was it?

Of course in its favour, VideoCrypt has recovered from some of these hacks. The problem is that VideoCrypt has to recover from each hack. Perhaps the situation has changed so that VideoCrypt now has to tolerate an “acceptable level of piracy”.

Case Study: Videocipher II

Video Scrambling: H and V Synch Replacement, video inversion

The horizontal and vertical synch pulses are removed and replaced with digital data. The video is inverted and the color burst is moved to a non-standard voltage level. This is primarily to stop certain brands of television receivers locking the video using the color burst.

Audio Scrambling: DES Encrypted Digital.

The audio is transmitted in 14 bit packets. Quad level Pulse Amplitude Modulation is used to transmit the data.

*Users: *** de facto US Standard ****

VideoCipher II is perhaps the most important scrambling system in the history of signal security. It marked the first attempt to have a system accepted as the de facto system for video scrambling. It was a good scrambling system except someone left the critical data in the decoder totally exposed. It was based on the technology of the early eighties but it rapidly underwent upgrades and modifications to improve security. This has been a largely up hill battle as it seems as soon as an upgrade is made to the system, there is a hack to counter it.

The VideoCipher II system applied hard digital encryption techniques to the digitised audio. The encrypted digital audio was then inserted into the video line in place of the synch. The VideoCipher I system applied digital encryption to the video and the audio but was only used for studio and inter-company video hook-ups. It wasn't really financially viable for the mass market that VideoCipher II was intended to serve.

The digital encryption technique used for encrypting the data was the Data Encryption Standard algorithm. The algorithm is reversed by the American National Security Agency every day. There is no evidence to suggest that it was reversed to hack the VideoCipher system - there were easier ways of hacking VideoCipher II. I have included an explanation of the DES format in Chapter Six as it is used in the VideoCipher system. It is essential to the understanding of the VideoCipher and the EuroCypher system.

The decoder had a tier mask. This can be thought of as a number of registers that would hold a bit for each channel. If the decoder was enabled for a channel the register would high and the decryption circuitry would be allowed to decrypt the signal. If the bit was low then the decryption process would be inhibited.

The weakness was that if you had the monthly key then nothing else was required. The program in U30, the EPROM was overwritten so that the tier mask was ignored. Since there was no tier mask check, all of the tiers were valid and the decoder was free to decode anything on that service.

GI naturally were able to countermeasure this hack. Indeed their financial lives depended on it. By sending some instructions over the air, it was possible to get the secure processor to compare the programme's tier mask with that of the decoder. If they did not match then the decoder halted.

Preview Bit Hack

Another hack was the use of the Preview Bit in the tier mask. Sometimes, channels would allow the decoder user to have a quick look at what he or she was missing. The Preview Bit allowed the decoder to the descramble the signal for a few minutes. Often the audio was decrypted and a the screen was blacked out and a barker message was displayed. By using a simple video decoder to descramble the video and the VideoCipher II decoder to descramble the audio, it was possible to get a clear service. Unfortunately, once GI found out, this loophole was plugged.

Clone Hack

The simplest hack on the VideoCipher II system was the clone hack. It extracted the decoder address and key set from a valid decoder and loaded them into other VideoCipher descramblers. As long as the original decoder or Clone Master remained authorised, all of the clones operated as well.

When GI found a clone master, they were able to knock out hundreds of clones in one go. The one thing that they were looking for was a decoder that was subscribed to all services. This aroused their suspicions.

Some of the clone hacks only wrote the key set to the battery backed up RAM. This left the original key set and address in the Secure Processor (TMS7000). One of GI's countermeasures was to check that the sets were the same.

The Wizard Hack

This was the most elegant hack on VideoCipher II. It allowed the direct entry of the monthly key from a key pad. The keys were available on bulletin boards, in hacker newsletters and on answering machines. Of course this type of key distribution is now illegal in the United States. The sources for the keys are outside the USA.

The McCormac Rating

As a shark can sense blood so can a good hacker sense a weakness in a system. It is a rather dramatic way of putting it. The abject fear and terror that seizes a channel executive when their system is hacked is like a scene from "Jaws". The channel executive almost always pictures themselves as the flailing, threshing victim with their viscera and lifeblood oozing out. Except their lifeblood in this case is cash and the viscera the programming.

The McCormac Rating is based on three areas of a system; the video scrambling, the audio scrambling and the access control system. Essentially it is a guide to the hackability of a scrambling system

Each aspect of the system is assigned a code. The first is a letter and the second is a number. The letter identifies the type of scrambling digital, (D) or analogue (A).

The second part of the rating is a number from one to nine. The lower the number the higher the security. The breakpoint on the scale is five. At this point the descrambling circuitry has to be a clone of the official descrambler. With the ratings from three to one, only the official descrambler circuitry can be used. It is not economical to clone it. For ratings greater than five, it is possible to use alternative circuitry instead of the official descrambler circuitry.

Video Scrambling

The security of the video scrambling system is based on a 1 to 9 scale. The higher the number the less the security. If the rating is greater than five then it is possible to build an alternative video descrambler. If the rating is lower than five then the official descrambler circuit has to be used. A figure higher than 7 means that the video scrambling system is totally compromised.

Audio Scrambling

The security of the audio scrambling system is based on a 1 to 9 scale. The higher the number the higher the risk of hacking. If the rating is greater than five then it is possible to build an alternative audio descrambler. If the rating is lower than five then the official descrambler circuit has to be used. Again a rating above seven means that the scrambling is totally compromised.

Access Control System

The code for the security of the access control system works in a similar fashion. In this case, the letter identifies the type of access control system in use. An over the air system is designated O. A smart card only system is designated S. A dual over the air - smart card system is designated D.

In many cases where the video and audio scrambling have been compromised it is not necessary to hack the access control system. Therefore it might well be that the access control system will be still intact even though the scrambling system is totally compromised. This is the situation with Discret. Of course the opposite case is also valid. The video and audio scrambling may have strong ratings but the access control system has been compromised.

There naturally will be some disagreement over the ratings assigned to each system. The main guideline is whether or not a system has been hacked. The McCormac Rating's approach is from the hacking angle. The manufacturer's publicity department can print as much purple prose as they like, it will not stop the system getting hacked, if indeed it is hackable. The following tables give the actual meanings of each rating. The table for the video and audio scrambling is identical.

McCormac Rating - Video And Audio

The Letters:

A: Analogue
D: Digital

The Numbers:

1 Totally Secure At This Time
2 Very Secure
3 Would Not Survive Complete Reverse Engineering
4 ODH Using Outboard Circuit to Effect Hack
5 Official Descrambler Required For Hack (Simple)
6 Reverse Engineer Of Parts Of Official Descrambler Required
7 Slightly More Complex but still hackable
8 Easily Hackable
9 Totally Compromised

McCormac Rating - Access Control

The Letters:

O: Over The Air Addressing
S: Smart Card Only
D: Dual System - Smart Card And Over Air Addressing

The Numbers:

1 Totally Secure At This Time
2 Very Secure
3 Would Not Survive Complete Reverse Engineering
4 ODH Using Outboard
5 Official Descrambler Required For Easy Hack
6 Reverse Engineer Of Parts Of Official Descrambler Required
7 Slightly More Complex but still hackable
8 Easily Hackable
9 Totally Compromised

The systems listed in the last version of the book have largely disappeared. As a result, only a generic listing for each of these systems is included.

In certain cases, channels have changed their scrambling systems. The most apparent of these is the FilmNet channel who changed from SATPAC to EuroCrypt.

SATPAC

System Name: Matsushita
Start Date: 01/Sept/1986
End Date: 06/Dec/1993 (Switched to EuroCrypt)
Audio Type: Digital
Video Inverted: Yes
Video Field Inversion: Yes (Upgrade 1)
Alternate Field Inversion: Yes (Upgrade 1)
Horizontal Synch Suppression: Yes
Field Synch Suppression: No
Pulse Suppression: Yes
Digitised Audio: Yes, Started June 1991
Digital Audio Crypto: Non-Standard
Origin Of System: Japan (Matsushita)
Descrambler Addressing: Yes
Known Hacks: Elektor Magazine Descrambler, various commercial descramblers. Hi-Tech are the only ones to have hacked the digital audio.
Date Video Hacked: 01/Sept/86, 24/March/1987, 24/12/89, 05/11/90
Date Audio Hacked: January 1992

The scrambling in this system is based on a field inversion sequence. As a result it is relatively simple to hack. There are only thirty two sequences and it is based on a 16 field sequence. This was a totally compromised system. FilmNet had tried to introduce digital audio but in the end it was only an interim fix until they went to D2-MAC EuroCrypt.

McCormac Rating:

Video: A9

Audio: D6

Control: O7

SAT-TEL SAVE

System Name:SAT-TEL SAVE
Start Date: 04/June/1987
Audio Type: Spectrum Shift
Video Inverted: Yes, half normal level
Sine Suppression: Yes, 93.3 KHz approx.
Origin Of System: Telease MAAST (USA)
Descrambler Circuit Known: Yes
Availability Of Official Descramblers: Outside UK
Date Hacked: 04/June/1987, May/1989

The SAVE system was used by a number of broadcasters until recently. It is a very low security system. Various options such as multifrequency sinewave and audio scrambling were available though even these were quickly hacked.

McCormac Rating

Video Scrambling: A8

Audio Scrambling: A6

Access Control: N/A

Oak ORION

System Name: OAK ORION
Start Date (Europe): 1982, Clear Spring 1988
Audio Type: Encrypted Digital (USA)
Video Line Inversion: Yes
Video Field Inversion: Yes
Random Line Inversion: Yes
Alternate Line Inversion: Yes
Alternate Field Inversion: Yes
Horizontal Synch Replacement: Yes
Field Synch Replacement: Yes
Digitised Audio: Yes, Encrypted
Other Users Of System: Various Cable Nets
Descrambler Circuit Known: Yes
Availability Of Official Descramblers: Cablenets and SMATV
Custom ICs Used: Yes
Function Of Custom ICs: Audio Decryption / Access Control

Descrambler Addressing: Yes
Known Hacks: Elektor Magazine Descrambler, USA
Date Hacked: Video Only 1982, USA EPROM Hack 1987

This system was the forerunner of the IRDETO and LuxCrypt systems. Its most devastating hack was the EPROM hack. It was possible to insert an EPROM in place of the official ROM and access channels. In Europe there was no need for such a hack. It was only employed as a video scrambling system. The audio was clear.

This is an old system but is one of the better examples of system design. However the fact that it could be hacked tended to work against it.

McCormac Rating

Video Scrambling: A7

Audio Scrambling: D3

Access Control: O5

RTL4-Veronique / LuxCrypt

System Name: Luxcrypt
Start Date: 05/02/90
Audio Type: Clear
Video Inverted: Possible though not used.
Video Line Inversion: Possible
Video Field Inversion: Possible
Random Line Inversion: Possible
Alternate Line Inversion: Possible
Alternate Field Inversion: Possible
Horizontal Synch Replacement: Yes
Field Synch Replacement: Yes
Digitised Audio: Yes but unused
Origin Of System: IRDETO
Descrambler Circuit Known: Yes
Availability Of Official Descramblers: RTL4-V area only
Descrambler Addressing: Not used
Known Hacks: Multiple
Date Hacked: 1989

This is the lowest level implementation of the IRDETO system. the audio scrambling and encryption is not used. This implementation is essentially a token scrambling of the signal.

McCormac Rating

Video Scrambling: A8

Audio Scrambling: N/A

Access Control: N/A

Payview III

System Name: Payview III
Start Date: 1989 (Teleclub have switched to Syster)
Audio Type: Possible digital format but unused in tests
Video Inverted: Yes
Video Line Inversion: Yes
Video Field Inversion: Yes
Random Line Inversion: Yes
Alternate Line Inversion: Yes
Alternate Field Inversion: Yes
Horizontal Synch Suppression: Blanking level and colour burst raised over peak white level.
Line Delay: Pseudo line delay effect by misplaced line synch
Digitised Audio: Yes, but not used in tests.
Origin Of System: Hong Kong
Other Users Of System: None Known
Descrambler Circuit Known: Yes
Custom ICs Used: Unknown
Function Of Custom ICs: Unknown
Descrambler Addressing: Possible
Date Hacked: 1989
Known Hacks: Multiple

The system was hacked using a number of methods. The video is easy to hack on its basic level. There are a number of problems that can arise with the active video inversion. While the sequence is generally field based, the actual sequence is changed every few months. This can cause problems for some of the microcontroller

based descramblers. Commonly it is an EPROM fix. Some of the more advanced Teleclub descramblers use video polarity detection on a line by line basis.

McCormac Rating

Video Scrambling: A6

Audio Scrambling: N/A

Access Control: N/A

Canal Plus / RITC Discret 1

System Name: RITC Discret 1
Start Date:1984
End Date: 1990
Audio Type: Spectrum inverted
Line Delay: Yes, 0 nS, 902 nS and 1804 nS
Audio Spectrum Inversion: Yes, 12.8 KHz carrier frequency
Origin Of System: Europe
Descrambler Circuit Known: Yes
Availability Of Official Descramblers: France
Custom ICs Used: Yes
Function Of Custom ICs: Access Control
Descrambler Addressing: Yes
Known Hacks: Radio Plans Descrambler, Various microcontroller versions.
Date Hacked: 1984, September 1987

The system initially used one filler. The upgrade used three at the beginning and end of lines. This upgrade defeated many of the hacker descramblers. Of course it did not last very long.

McCormac Rating

Video Scrambling: A7

Audio Scrambling: A9

Access Control: O4

RAI / RITC Discret 12

System Name: RITC Discret 12
Start Date: 1990
Audio Type: Spectrum inverted
Line Delay: Yes
Audio Spectrum Inversion: Yes, 12.8 KHz carrier frequency
Origin Of System: Europe
Descrambler Circuit Known: Yes
Availability Of Official Descramblers: Unrestricted
Custom ICs Used: Yes
Function Of Custom ICs: Access Control
Descrambler Addressing: Yes
Known Hacks: Multiple
Date Hacked: 1989

The system uses the DIGIT 2000 series of IC from ITT digitise the video. The delays are introduced using shift registers. The abundance of pirate descramblers is a testament to the system's security or rather the complete lack of it.

The video scrambling is slightly tougher than Discret 1. However this system is still totally compromised as regarding the availability of pirate descramblers. Its use on terrestrial networks would be dangerous but as its use on satellite transmissions declines, the availability of pirate decoders on the open market would similarly decline.

There are reports that some MMDS nets in Ireland have started to use this system. The most obvious reason being that they got a good deal as regards the costs of the decoders and that their coverage ensures that piracy would be minimal.

McCormac Rating

Video Scrambling: A6

Audio Scrambling: A9

Access Control: O4

VideoCrypt

System Name: VideoCrypt
Start Date: 05/02/90
Video Scrambling: Cut And Rotate On Video Line.
Audio Spectrum Inversion: Not Implemented
Origin Of System: Thomson, Europe. News Datacom
Other Users Of System: JSTV, TV-Asia, The Ault Channel
Descrambler Circuit Known: Yes - See Chapter 7
Availability Of Official Descramblers:UK And Ireland
Custom ICs Used: Pseudo Random Sequencer / Clocking
Function Of Custom ICs: Control / Sequencing
Descrambler Addressing: Over The Air Exclusion principle.
Known Hacks: Voltage Interrupt, McCormac Hack, KENtucky Fried Chip, Ho Lee Fook, OMIGOD, DDT
Date Hacked: 1990, 1991, 1992, 1993, 1994

It is more or less the standard English language scrambling system on ASTRA. Each decoder requires a Smart Card to function. It is beginning to show its age with a barrage of continual hacks.

McCormac Rating

Video Scrambling: D2

Audio Scrambling: N/A

Access Control: D9

Note: The reason that this system's rating is designated D9 is because the DDT hack still works. It is possible to record the keystream from a valid card decoding a programme and then play back that keystream and a tape recording of the programme through the decoder.

The decoder will decode the scrambled program. This effectively knocks out a viable PPV option with programmes like movies rather than sporting events.

VideoCrypt-S / BBC Select

System Name: VideoCrypt - S
Start Date: 1992
Video Scrambling: Block Line Shuffle
Audio Spectrum Inversion: Intermittent
Origin Of System: Thomson, Europe. News Datacom, BBC
Descrambler Circuit Known: No
Availability Of Official Descramblers:UK
Custom ICs Used: Control Logic / Sequence,
Function Of Custom ICs: Control / Sequencing
Descrambler Addressing: Over the air exclusion principle.
Possible Hacks: Voltage Interrupt, McCormac Hack, KENtucky Fried Chip

Each descrambler requires a Smart Card to function. It is a more secure system than VideoCrypt but it is still vulnerable to the same hardware hacks. The reason that no work has been carried out on hacking it is due to the rather small number of viewers that have decoders.

McCormac Rating

Video Scrambling: D2

Audio Scrambling: A8

Access Control: D3

Videocipher II

System Name: Videocipher II
Start Date: 1985
Audio Type: 14 Bit QAPM Encrypted using DES
Video Inverted: Yes
Horizontal Synch Replacement: Yes
Field Synch Replacement: Yes
Digitised Audio: Yes
Origin Of System: M/A Com, USA
Descrambler Circuit Known: Yes
Custom ICs Used: Yes
Function Of Custom ICs: DES Processor (TMS7000 uController)
Descrambler Addressing: Yes

Known Hacks: Musketeer, Preview Bit, Combo, Wizard
Date Hacked: June 1986

The system was hacked using a number of methods. With the continuing upgrade policy, the system security oscillates between being totally compromised and temporary high security. It is due to be replaced with VideoCipher II Plus and RS.

McCormac Rating

Video Scrambling: A9

Audio Scrambling: D2

Access Control: O5

Note: Given the transition to the VideoCipher II Plus, the lifetime of VideoCipher is probably very limited. There are rumours concerning the VC Plus hacks. The problem is that there is a very effective legal framework in the USA to deal with piracy.

As a result many potential pirates are entrapped by operations by US Customs and other official departments. Some pirates have been extradited from Canada and other jurisdictions to stand trial in the USA for piracy.

The satellite press in the USA, apart from the honourable exceptions of Scrambling News and Satellite Watch News, appear to be only interested in advertising and not upsetting GI et al. As a result there is very little research into the systems in the mainstream press. Indeed some of the stuff that appears in the mainstream press is just a rehashed press release from system manufacturers.

Nagra Kudelski Syster

System Name: Syster / Nagravision
Start Date: 1991
Video Scrambling: Block Line Shuffle, Sliding Bar Shuffle, Line Cut And Rotate, Line Delay.
Origin Of System: Nagra Kudelski, Switzerland
Descrambler Circuit Known: Yes
Availability Of Official Descramblers:Canal Plus Areas
Custom ICs Used: Control Logic / Sequence,
Function Of Custom ICs: Control / Sequencing
Descrambler Addressing: Over The Air And Smart Card
Smart Card: The shape of the card is unusual. It is key shaped rather than card shaped. It is, however, smart.

Notes: This is one of the more secure systems in that its video scrambling is a chameleon type. There are apparently two different flavours of this system: one is a line shuffle version and the other uses line shuffle and cut and rotate.

The system has been used in Germany and Spain. In the German application, only line shuffle appears to have been used so far. Line shuffle and cut and rotate techniques have been used on the Spanish service.

This system is arguably the most widespread European system as when it is fully deployed it will have at least 5 Million users. An estimated 3.7 Million of the users will be Canal Plus France subscribers.

There have been rumours of hacks on this system but nothing concrete has been seen. One of these rumours concerned a dual circuit unit that allowed the video to be descrambled.

McCormac Rating

Video Scrambling: D1

Audio Scrambling: N/A

Access Control: D2

Tele Piu / IRDETO

System Name: IRDETO
Start Date: 1992
Audio Type: Encrypted Digital
Video Line Inversion: Yes
Video Field Inversion: Yes
Random Line Inversion: Yes
Alternate Line Inversion: Yes
Alternate Field Inversion: Yes
Horizontal Synch Replacement: Yes
Field Synch Replacement: Yes
Digitised Audio: Yes, Encrypted
Other Users Of System: Various Cable Nets
Descrambler Circuit Known: Viideo Only
Availability Of Official Descramblers: Copyright area only
Custom ICs Used: Yes
Function Of Custom ICs: Audio Decryption / Access Control
Descrambler Addressing: Yes
Known Hacks: Video - Elektor Magazine Descrambler
Date Hacked: Video Only 1992

The IRDETO system is the one from which LuxCrypt is derived. It has digital audio encryption whereas LuxCrypt only uses the video scrambling section.

The audio decryption and access control are ASICed. To date there has not been enough interest in the system to warrant a reverse engineering of the ASIC. Therefore the audio and access control elements are still intact.

McCormac Rating

Video Scrambling: A7

Audio Scrambling: D3

Access Control: O3

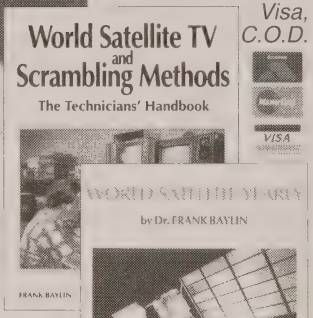
Baylin Publications

ALL ITEMS EX-STOCK.

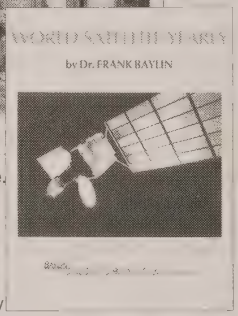
24 River Gardens, Purley, Reading.
RG8 8BX. England.
Tel/Fax 0734-414468
Mobile 0836-582785

Pay by: UK£ cheque, Access, Mastercard, Visa, C.O.D.

Ku Band Satellite TV, Theory, Installation & Repair 4th Edition. Footprints, dish theory, cables, site survey, polar mount adjustment. ***£25.***



European Scrambling Systems, Circuits, Tactics & Techniques. By John McCormac, digital sound, smart cards, pirate decoders, for hackers. 4th Edn. ***£32.***



World Satellite TV & Scrambling Methods. 3rd Edition, by Baylin, Madox & McCormac for the service engineer. ***£29.***

Home Satellite TV Installation Videotape. Forty minutes VHS Pal. See how 3 metre dishes are installed. ***£27.***

Satellite Installation Guide. 3rd Edition. By John Breeds. ***£15.***

The Satellite Book. 3rd Edition. A complete guide to satellite TV . Theory and practice by John Breeds. ***£32.***

TVRO System Analysis and Aiming Software. 5.25 or 3.5 disk, (DOS 3.2). Calculates dish size and lists coordinates of all satellites in view. ***£39.***

Satellite Toolbox Software, for IBM Comp. Hard Disk– 5.25 or 3.5. ***£59.***

Wireless, Cable & SMATV, Microwave broadcasting & cable TV. ***£35.***

World Satellite Yearly by Dr. Baylin, Loading and 200 Footprints. ***£59.***

PRICES INCLUDE P. & P. UK. Airmail Europe add 10%. Outside Europe + 30%.

Descrambler Building Blocks

Over the last few years the Blackbox industry has switched from completely analogue scrambling systems to digitally based systems. There are a few of the old analogue scrambling systems left in operation. As a result of this most of the basic building blocks in this chapter have been left in for this version. A representative circuit for each system is also given.

The biggest change from that last edition is that this chapter has been expanded to cover smart cards. The main reason for this is that many of the present and recent hacks have been smart card based.

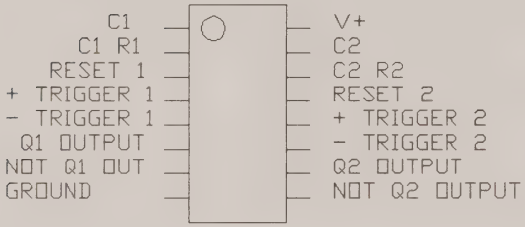
The circuits given in this chapter are those most commonly used by hackers. CMOS circuitry is almost invariably used as it is almost totally noise immune. This can be a good advantage to have when the receiver is microprocessor controlled as indeed are most ASTRA receivers. TTL circuitry is not generally used as it is too current hungry. There is a growing trend to use the low power fast TTL for crystal oscillator applications.

Monostables

Most of the simple analogue scrambling systems interfere with the synch section of the video signal. It is therefore essential for the hacker to regenerate the synch pulses. The most versatile circuit for this operation is the monostable multivibrator. The NE555 may sound like a good choice but it is not. It does not offer the designer or hacker the same facilities as the gated monostable multivibrator.

The commonest circuit in hacking for timing purposes is the gated monostable multivibrator. Hackers mainly use three versions of this circuit; the 4098, the 4528 and the 4538. The 4538 is the precision version and is rarely used in low cost descramblers. Each IC contains two monostables. The timing constant for each monostable is set by an RC network. Each monostable can leading edge or trailing edge triggered. There are two outputs Q and NOT Q. The formulae for the timing constants are given with the circuit diagrams. Precision components such as silver mica or polystyrene capacitors and metal film resistors are recommended. If precision resistors are not available

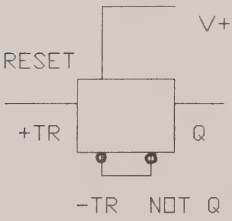
4098,4528,4538 Monostable



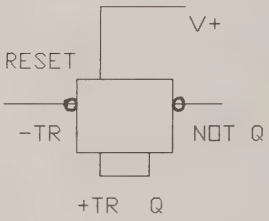
Formulae;
T=0.5(RC)
4098,4528
T=0.7(RC)
4538

T is in Seconds
R is in Ohms
C is in Farads

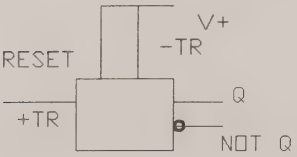
Leading Edge
Non-Retriggerable



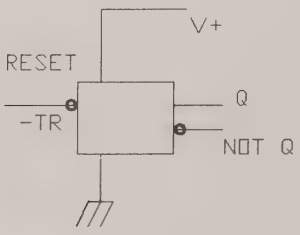
Trailing Edge
Non-Retriggerable



Leading Edge
Retriggerable



Trailing Edge
Retriggerable



then a carbon film-preset combination should be used. These circuits are the cornerstones of hacker descramblers. Ceramic capacitors should not be used for setting timing constants as they tend to drift causing severe synching problems.

Comparators

With many scrambling systems, it is necessary to detect a particular voltage level. This voltage level generally triggers some timing or processing circuitry. When the voltage level is part of the video signal, the video signal is normally amplified. The 311 comparator IC is then used to check the signal against a known reference level. The preset on the reference input, (see circuit), is always a multiturn cermet type. The comparator is also used as a Schmitt trigger to clean up pulses. In some cases two or more comparators will be required. In these cases the 339 quad comparator is used. This IC is cheaper than the twin comparator and so will probably be used if only two comparators are required. The pinouts for both ICs are given in the application diagram.

In FilmNet descramblers, comparators were used to clean up the synchs or detect the polarity of the video using the horizontal synch. Other descramblers such as those used on the Discret system use the comparator to detect the start of video in each line. This is accomplished by sampling the black level with a sample and hold circuit. The sampled level is then compared to the video signal.

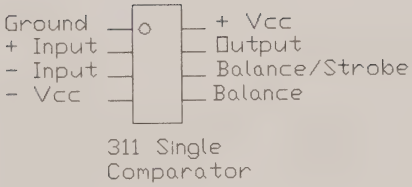
Synch Insertion And Restoration

There are many methods of reinserting or restoring the synch pulses in video signals. The circuits covered here are the most widely used. In some cases such as the LuxCrypt system, it is necessary to completely recreate the synch pulses.

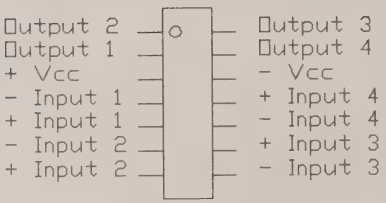
Two Amps - One Clamp:

A simple two amps-one clamp circuit can be used to pull the synch down to its proper level. This type of circuit can only be used to restore the synch to its proper level, it cannot be used to reinsert a synch pulse.

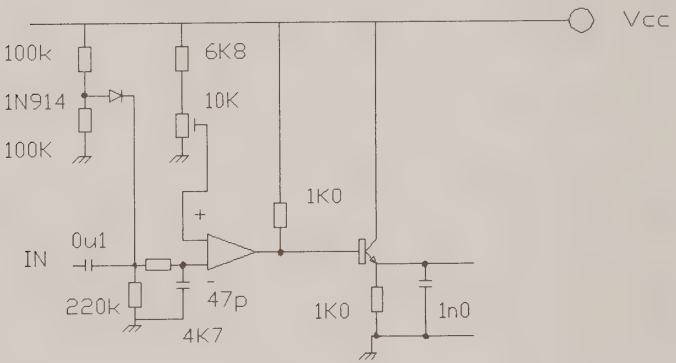
A refined form of the two amps-one clamp is used by the more advanced hacker. This circuit was first published in “Elektor Electronics”.



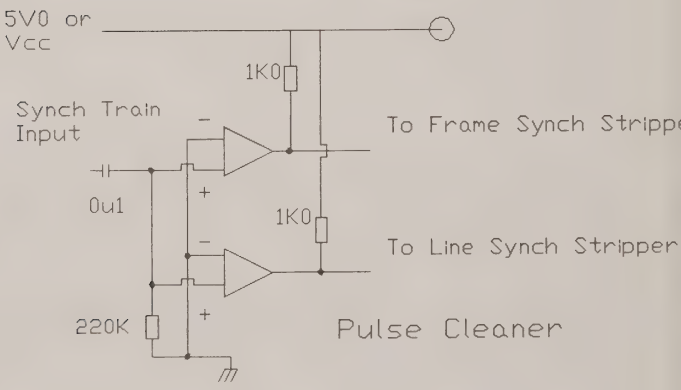
311 Single Comparator



339 Quad Comparator



Synch Stripper



Pulse Cleaner

The Multiplexer Approach:

This circuit allows the black level and the synch tip level to be re-inserted. The voltage levels of the blanking and synch tip are set by presets. The multiplexer switches off the video and switches in the correct voltages to restore the synchs.

The commonest IC for this purpose is the 4051 one into eight multiplexer. The normal and inverted video signals are connected to two inputs. The black level and synch tip levels are connected to two other inputs. Some external logic circuitry controls the addressing pins.

The application circuit is shown with an NE592 video amplifier connected to give positive and inverted video into the multiplexer.

This type of circuit is most useful in applications that requires either a polarity key or digital audio information to be separated from the scrambled waveform. The circuit can be implemented using the 4066 or 4016 CMOS switches instead of the multiplexer.

Miscellaneous CMOS Circuits

CMOS Integrator:

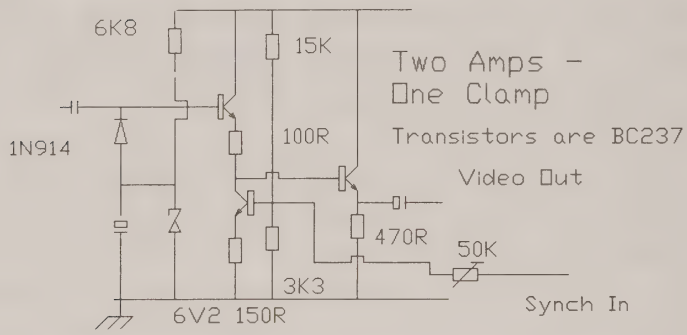
CMOS circuitry can be used in analogue applications. A CMOS inverter can be made to function as an operational amplifier. In some applications, an integrator circuit is required. A typical circuit block using CMOS inverters as op-amps is given along with circuit values. This particular circuit has been used in the monostable Filmnet descrambler design to separate the frame pulse from the synch signal transmitted on the 7.56 MHz carrier.

The addition of a 100K resistor across the second capacitor can improve the operation of the integrator. The values are not extremely critical.

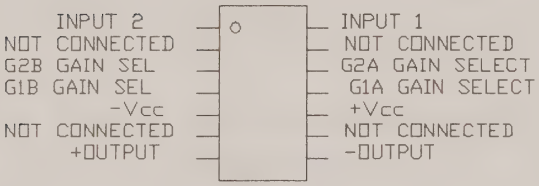
CMOS Monostable Using NOR Gates:

In order to protect a descrambler design from reverse engineering, a hacker most often resorts to unusual design techniques. The most obvious choice for a monostable is the 4528. With this circuit, NOR gates are used to function as a monostable. It can be used for general applications where precision timing is not necessary.

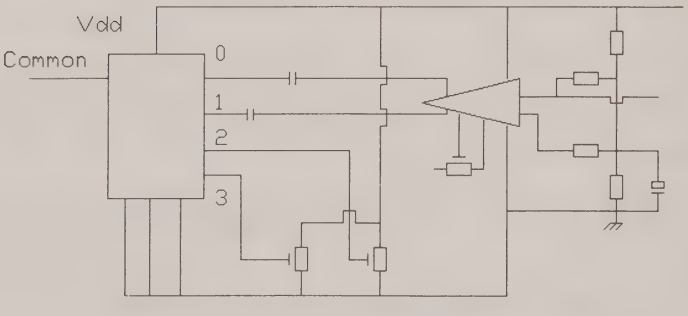
Synch Insertion Circuits



(Circuit Courtesy Of Elektor)



NE592 / uA733 Video Amplifier



INH, Vee, Vss
Mux= 4053 or 4051

BLANKING LEVEL AND
SYNCH TIP LEVEL PRESETS

Multiplexer Synch Inserter

Composite Synch Demodulators

With external synch carriers, a separate demodulator is required. There are many circuits available for such a demodulator. The Filmnet SATPAC system was a good example of a synch carrier system. Most of the commercial pirate descramblers used a TBA120 for the demodulation of the carrier. Generally there is a tuned filter prior to the TBA120. This naturally adds to the setup costs. On some of the better quality pirate descramblers, the 7.56 MHZ carrier is upconverted to 10.7 MHz where it is passed through a standard 10.7 MHz ceramic filter. Tuning this type of demodulator is easier as it only means adjusting a tuning preset.

A further simplification is the use of a crystal based oscillator to provide the mixing frequency. The frequency used is generally high side, (18.26 MHz). This approach was used in the Hi Tech Xtravision FilmNet descrambler.

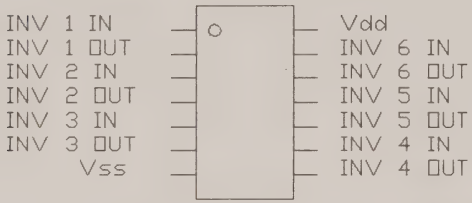
The cable version of the FilmNet system modulated the synch carrier on to the FM audio subcarrier. Most of the pirate designs worked by detecting this synch signal and using a PLL. Of course the difference here was that the processing would have been better handled at RF. Some television sets tended to clamp the video and as a result the descrambled picture from a modified satellite type decoder was not as good as the RF version.

Polarity Detection

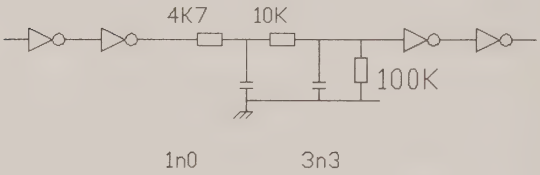
Video inversion is where the video section of the line is inverted but the horizontal blanking section of the line remains at normal polarity. It is difficult though not impossible to hack. There are is a number of weaknesses that allow the hacker to ascertain the polarity. The reason the system designers considered video inversion so secure was that they had not considered the widespread use of microcontrollers in descramblers. The microcontrollers allow the hacker to generate accurate time slots for sampling the video signal.

One possibility for defeating random video inversion is to digitise the a number of lines and compare the first few bytes at the start of each line. This may require a frame store to be properly effected. With some of the random line inversion systems, there is a signal transmitted in the line to tell the legitimate descrambler what type of scrambling to expect. This trigger signal is generally transmitted after the colour burst and before the video information. This reduces the security of the

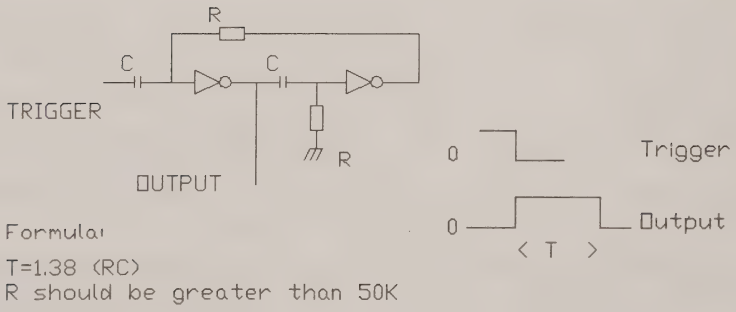
CMOS Inverter Circuits



4069 Hex Inverter and 40106 Hex Schmitt Inverter



CMOS Integrator (Frame Separator)

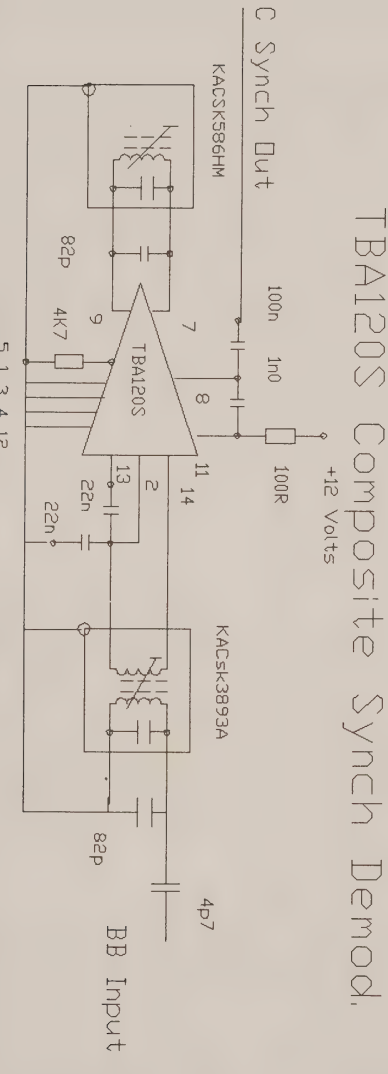


Formula:

T=1.38 (RC)

R should be greater than 50K

CMOS Monostable


TBA120S Composite Synch Demod.
C Synch Out
KACSK586HM
100n
1n0
100R
+12 Volts
82p
4K7
9
7
8
TBA120S
11
14
2
13
22n
22n
5 1 3 4 12
KACsk3893A
82p
4p7
BB Input

system and ensures that the system can be easily hacked. It should be remembered that most of the systems using video inversion were designed prior to 1985 and so reflect design ideas that are almost ten years old.

The vertical blanking interval is also used to transmit the sequence of the inverted line. Most of the companies using this technique seem to think that this method is secure against hackers. If the sequence is not encrypted they have or rather will have a critical problem on their hands. Normally one or more lines that would have been used for teletext are pre-empted for descrambler information. For a hacker, such a line would be easy to strip. A line snatcher circuit for oscilloscopes was published in "Elektor Electronics" magazine. The function of the circuit was to strip the vertical interval test signals for analysing the response of various television circuits and links. The circuit was presettable as to which line it snatched. It is extremely easy to convert this circuit to snatch the descrambler data.

Many of the early Teleclub descramblers sampled the black levels of the pre video lines in each field to ascertain the inversion sequence in use. This method was neutralised by Teleclub. A false sequence was incorporated in the pre video lines.

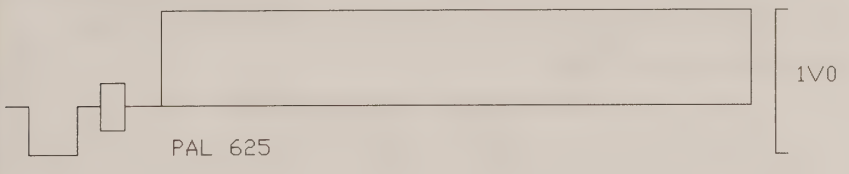
Sequence detection is one of the easiest hacks for the system owner to disable. Since the hacker descrambler is expecting a sequence of a preset duration, any variation in time of that sequence will upset the descrambler. A change of sequence will also defeat the descrambler. This method was used by Teleclub to defeat the switchable sequence descramblers. The sequence in these descramblers was set manually using a bank of DIL switches. By changing the inversion sequence inside a ten second period, it became impossible for the user to reset the sequence.

Line Inversion:

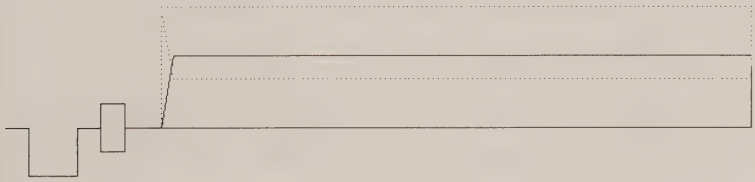
Line inversion is rarely used without synch suppression. The complete line is inverted. This is the easiest form of inversion to hack. The suppressed horizontal synch can be used as a key to determine the polarity.

This inversion type is used on the FilmNet system. As such is the most widely analysed type. The countermeasures adopted by FilmNet have been rather clever but were never totally successful. They were all hacked inside an hour.

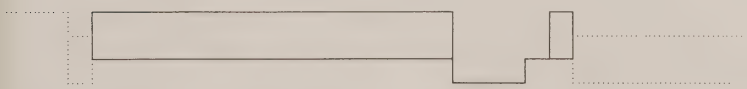
Polarity Detection - Inversion Types



Suppressed Synch With Complete Line Inversion.
Used by FilmNet.



Video Only Inversion On Clean Synch Signal.
The example shown has an inversion offset. This means that there is a DC offset between the inverted video and the normal video.



Field Based Inversion.
The inversion sequence can be pseudo-random, sequential or Average Peak Level based. The actual inversion point occurs in the VBI rather than in the vertical blanking pulse.

NOKEY Suppressed Synch Methods

A NOKEY system has no key that identifies the video as inverted or normal to the official descrambler. The inversion sequence is determined by an algorithm. The systems using this type of scrambling are generally addressable.

Comparative Level Detection:

The comparative level detection circuit compares a sample of the horizontal synch pulse tip with a sample of the horizontal blanking level. In a normal polarity signal the tip of the horizontal synch pulse should be lower than the blanking level.

The circuit is only active during the horizontal blanking period. The output of the circuit is used to trigger a flip-flop or a monostable. The output of the monostable or flip-flop controls the video multiplexer. The sample points can be derived from monostables or from a system clock. Most of the present FilmNet descramblers use clock derived slots.

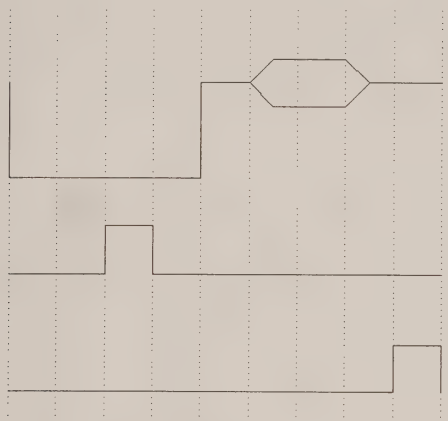
This is one of the most widely used methods of polarity detection on the FilmNet system. It can be defeated by placing a pulse at the point in the horizontal synch pulse where the sample is taken. The descramblers that used clock derived sample points were most vulnerable to this upgrade. This is one of the countermeasures that was used on the FilmNet system though it has been dropped because the descramblers were upgrade too easily.

Synch Tip Detection:

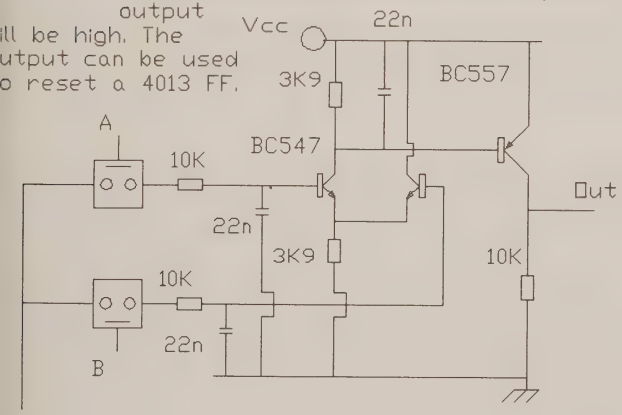
Synch tip detection is one of the easier types of level detection to implement. There is only one level to be detected. The detection occurs after the horizontal blanking section of the line has been pulled down to its normal level. If the polarity is correct then the level of the horizontal synch pulse tip should be at, or very close to, the clamp voltage. If the comparator detects a level greater than the clamp voltage then it will reset the flip-flop.

This type of polarity detector was first used in the Oak ORION descrambler design in the Pink And Brown Book. In that application it was used to detect the polarity key. Hi Tech Xtravision implemented this type of detector design in their FilmNet descrambler. The design differed from the Pink And Brown Book version in that it used CMOS rather than TTL. It is the most reliable method of polarity detection but it can be defeated.

Level Comparison Polarity Detection



If sample A is greater than sample B the output
ill be high. The
utput can be used
o reset a 4013 FF.



Video In

Capacitors should be metallised polyester types.

(Circuit Courtesy Of Elektor)

The FilmNet SATPAC upgrade of 05/11/90 was primarily intended to take out descramblers that were using this type of detector. The upgrade was a sine wave of near colour burst frequency. This had the effect of confusing the comparator. A later upgrade amplitude modulated the level of the sine wave using a very slow sine wave of approximately 1 Hz. This upgrade is similar to a facility in the IRDETO system. In that system, the digital audio level can be amplitude modulated by a 15 Hz sine wave. The circuit can be upgraded to cope with these countermeasures. It only requires the addition of two capacitors.

Energy Concentration Detection:

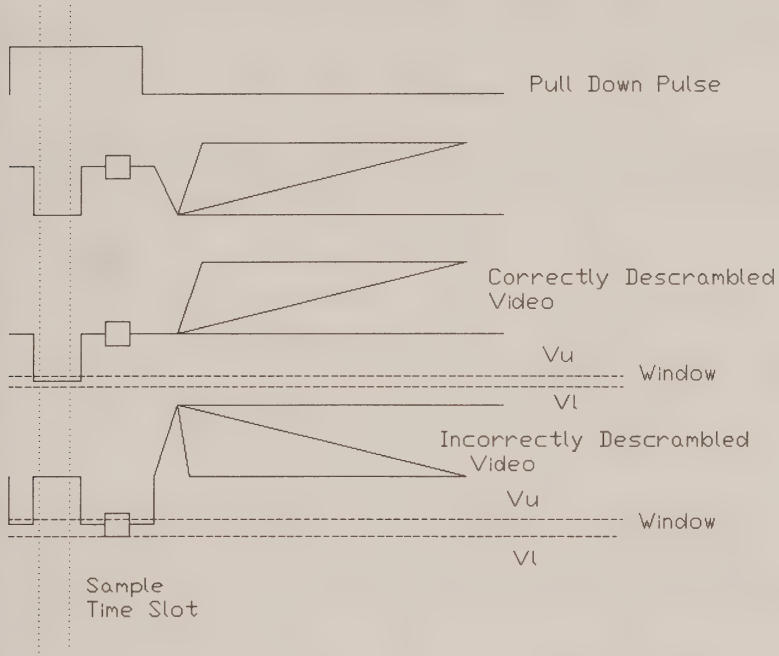
This is one of the more difficult methods to implement. It is also one of the more reliable. The energy level at the start of the video section of each line is sampled. If the level falls within the upper voltage window, the video is inverted. If the level falls within the lower window then the video is normal. The outputs of the comparators are fed to a logic circuit that controls the video multiplexer's monostable or flip-flop.

This type of detection generally requires a system clock in the region of 4 MHz. This is why many of the microcontroller based descramblers use it. It can be implemented by simpler circuitry.

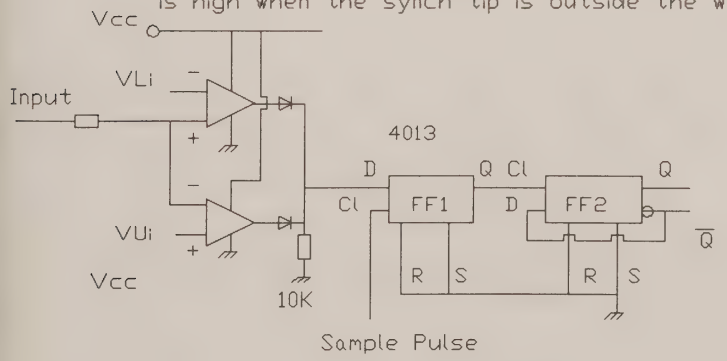
The colour burst generally remains in the same time slot in the scrambled video as it would in the normal video. The burst is used as the reference. This reference is used to lock a phase locked loop such as the 4046 to.

A monostable derived or logic time derived slot is then used to trigger the sampling circuitry. The logic derived solt is the preferred method. A triggered monostable can be trickier to set up in production as a capacitor and preset combination would have to be used to get the timing precise. Component aging and heating would also affect the monostable components thus changing the slot over the lifetime of the decoder. Ideally the phase locked loop will be running at a multiple of the line frequency. For a 500 nS slot, a clock frequency of at least 2 MHz would be required.

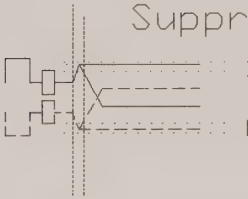
Synch Tip Based Polarity Detection



The circuit shown uses a window comparator to check the synch tip. The comparator output is high when the synch tip is outside the window.

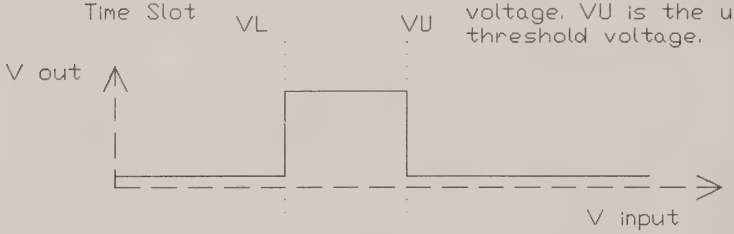


Energy Concentration Detection
Suppressed Synch Version

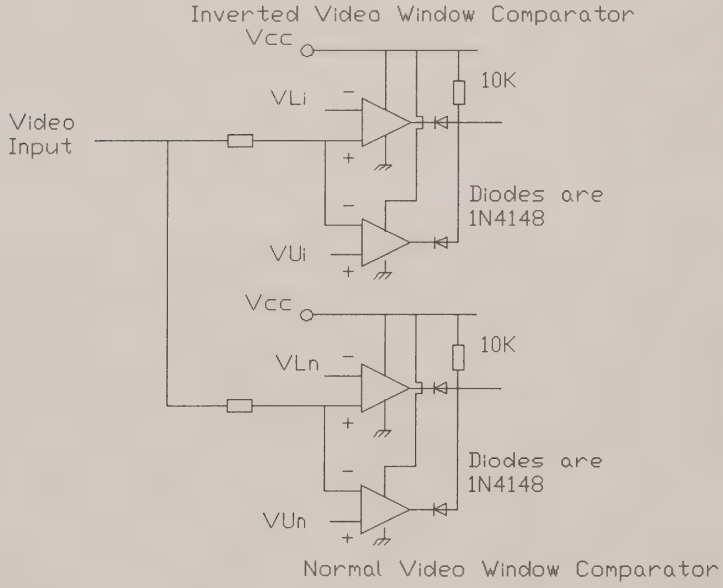


Sample Time Slot

VL is the lower threshold voltage. VU is the upper threshold voltage.



The output of the window comparator goes high when the input signal is between VL and VU.



KEYED Suppressed Synch Methods

A keyed system has a key that instructs the official descrambler as to the polarity of the video. It is a very insecure method and apart from the LuxCrypt and the OAK ORION systems, it is not really used any more.

Key Detection:

The circuits used for NOKEY polarity detection can be used for KEY polarity detection. The pirimary difference is in the timing of the sample slot. Most of the keys are after the colour burst and before the start of video.

Polarity Detection - Clean Synch methods:

Polarity detection is harder in clean synch systems. In a clean synch system, the synchs are not suppressed. If the designer knows what he is doing, he can make things very difficult for the hacker.

Energy Concentration Detection:

The same circuitry as used in the suppressed synch case can be used for this application. The timing reference can be the horizontal synch pulse or the colour burst. The burst is the more reliable of the two as the horizontal synch pulse can be dithered as in the PayView III system used by Teleclub.

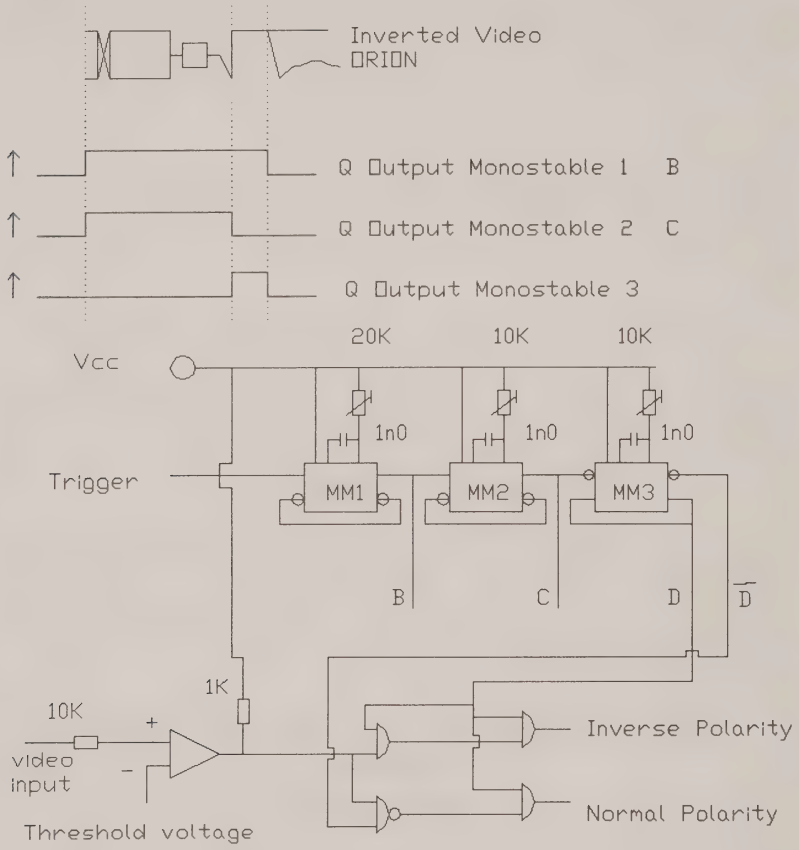
Line Video Delays And Pseudo Line Video Delays

Video Delays:

The delay of the video on a line by line basis is the basis of the Discret systems. There are a number of methods used to delay the video. The official Discret 1 descramblers used charged coupled device, (CCD), delay lines. The later PAL - SECAM Discret system used digital techniques to delay the video.

The delays used in the system were 0 nS, 902 nS and 1804 nS. The hackers of the Discret system used a colour transient improver IC, the TDA4560 to create the two delays required to hack the system.

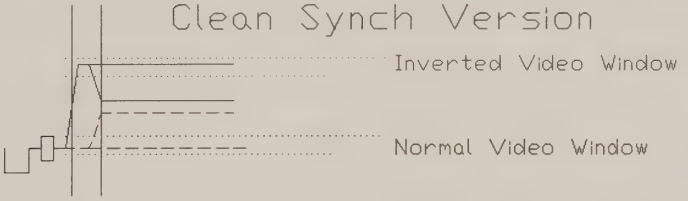
Polarity Key Detection



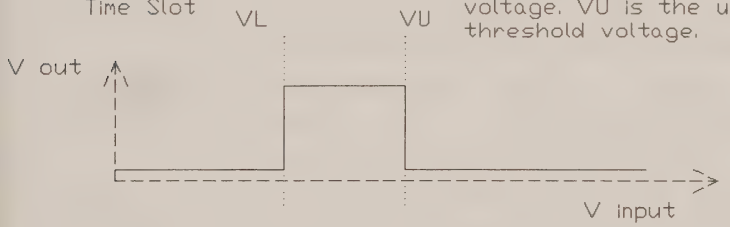
Monostable MM3 supplies the polarity key sample pulse. The comparator ascertains the state of the key and the logic only permits valid outputs when the sample pulse is present.

The trigger for the circuit is derived the line frequency output of a PLL.

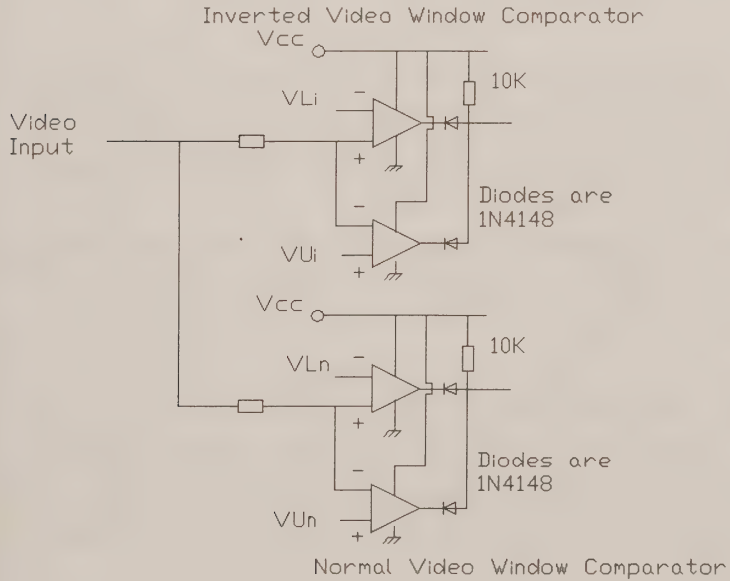
Energy Concentration Detection
Clean Synch Version



VL is the lower threshold voltage. VU is the upper threshold voltage.



The output of the window comparator goes high when the input signal is between VL and VU.



The TDA4560 contained a gyrator delay line that produced a delay of 888 nS. The TDA4565 has been superceded by the TDA4565. This IC is used in many of the descramblers used for the RAI service via Eutelsat.

The gyrator delay line in the TDA4565 can cope with signals up to 5.5 MHz without any serious degradation. The downside of the argument is that the IC has a through loss of 6 dB. This means that the video signal at the output has to be amplified by 6 dB. In the "Radio Plans" descrambler given in the case study, this amplification was achieved by using a TBA970. The NE592 could also be used for this purpose but it would require black level clamping.

Other attempts at fabricating delay lines were made. These ranged from custom glass delay lines that were manufactured by an Italian factory to a lumped inductor capacitor delay line.

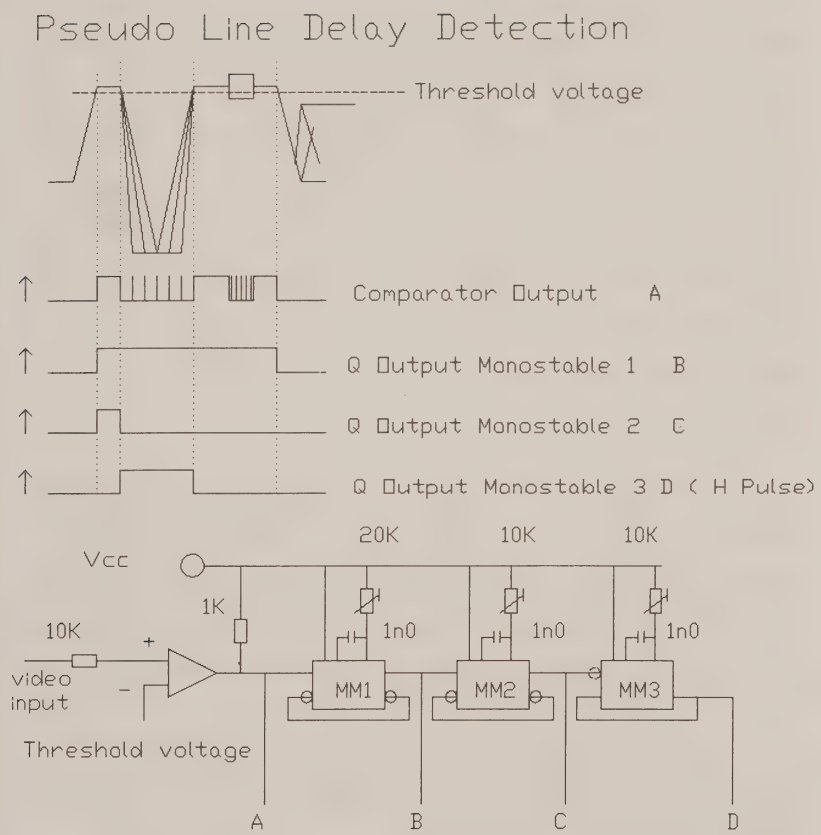
The digital approach to video delay was used by the official descramblers. They use a sampling frequency of four times the colour burst frequency, (17.735 MHz). This resulted in a cleaner picture definition on the descrambled picture.

Pseudo Line Delay:

This technique has to be one of the cleverest methods of not delaying the video. The horizontal synch pulse is shortened and dithered in the horizontal blanking area. This creates the effect of line delay but the video starts in te normal position. It is only the position of the horizontal synch pulse that changes.

Teleclub's old system, PayView III, had this facility. When used it had a 90% kill rate on the pirate descrambler market. The only descramblers that survived were those that re-inserted a new horizontal synch pulse.

While most of the pirate descramblers that survived used the colour burst slot as the timing reference, there were some that took a more novel approach. The horizontal blanking in the PayView III system is raised above peak white. By using a comparator to detect the rising edge of the transition to the raised horizontal blanking, a retimed and recreated horizontal synch pulse could be inserted in the horizontal synch pulse.


Pseudo Line Delay Detection
Threshold voltage
Comparator Output A
Q Output Monostable 1 B
Q Output Monostable 2 C
Q Output Monostable 3 D (H Pulse)
20K
10K
10K
Vcc
1K
10K
1n0
1n0
1n0
video input
MM1
MM2
MM3
Threshold voltage
A
B
C
D

Autoswitching

The term "autoswitching" means that the descrambler will detect a scrambled signal and descramble it automatically without the intervention of the user.

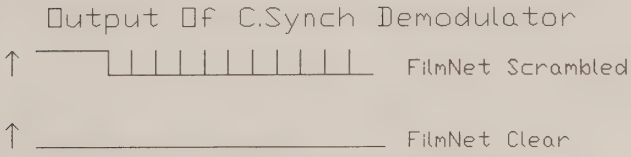
The descrambler will route the descrambled video to the return video input on the receiver or to the direct video input of a television. The SCART or the D-Type connector are commonly used on the ASTRA type receivers. These connectors have all the outputs and inputs necessary to interface a descrambler with the receiver. On ASTRA receivers there will be a descrambler SCART or D-Type. The descrambler SCART differs from the standard SCART. (Chapter 9 examines this topic in more detail.) In the case of a SCART or D-Type connector the descrambler must supply a switching voltage to control pin to make the receiver accept the descrambled video signal rather than the receiver demodulator output. When the standard SCART is being used to supply a television with the descrambled video, the same switching voltage at pin 8 on the SCART must be present. The voltage should be 12 Volts for external video and audio source selection and 0 Volts for internal select.

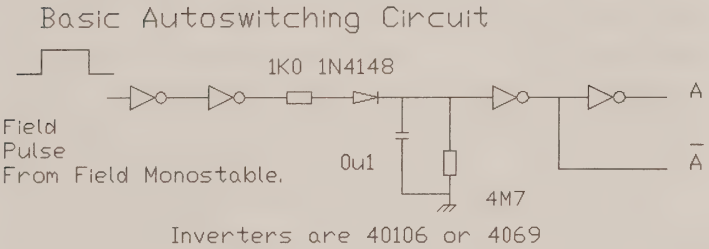
The detection of a scrambled signal is crucial to the autoswitching process. The official descramblers detect the addressing data in the scrambled signal. The Sky VideoCrypt descrambler will put up a channel identifier when it is fed with the scrambled Sky Movies signal. It also activates a switching pin on the descrambler scart to switch the decoder into the loop. Internal versions use a multiplexer to effect the switch over. Sometimes when this multiplexing IC blows there is no video on scrambled or clear channels.

The actual type of autoswitching control is very much dependent on the descrambler's operation. For a descrambler that uses a composite synch carrier technique, the circuitry is extremely simple. The FilmNet SATPAC system was a good example.

When FilmNet was scrambled the composite synch carrier at 7.56 MHz carried the composite synch signal necessary to descramble the signal. When the signal was not scrambled, the composite synch signal was not transmitted on the 7.56 MHz. The autoswitching circuit would have to detect the absence or presence of the composite synch signal. The main consideration is that the circuit doesn't trigger on an audio signal.

Autoswitching Techniques



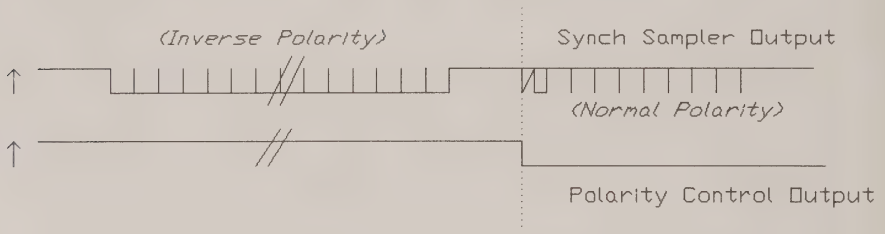


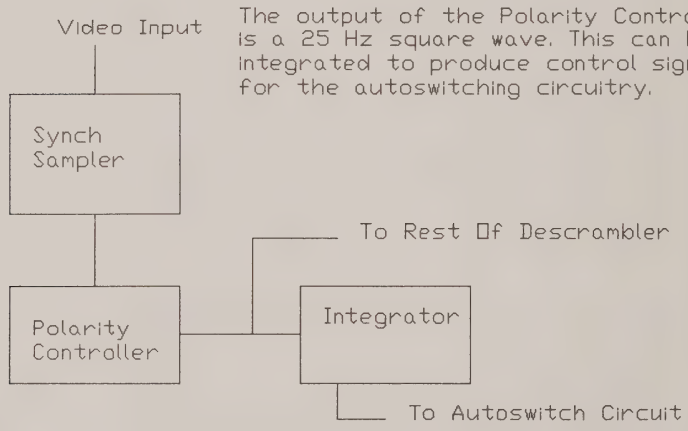
The outputs of the above circuit can be used to control the switching in the descrambler. The output A would be used to to control Pin 8 on the receiver's decoder SCART.

The output A is only high when there is a composite synch signal being transmitted on the 7.56 MHz s/c.

FilmNet could neutralise this form of autoswitching by leaving the composite synch on the 7.56 s/c even when the channel is clear. It is not known if the official descrambler uses this composite synch signal to switch in the descrambling circuitry.

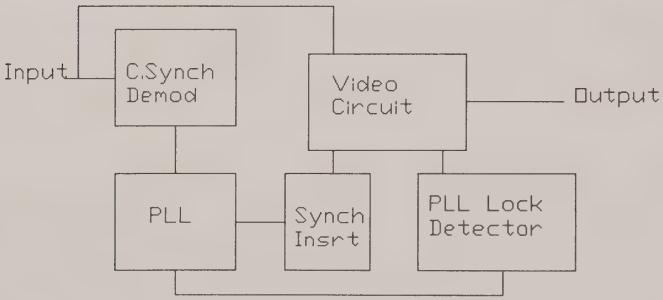
Autoswitching Techniques





The output of the Polarity Control is a 25 Hz square wave. This can be integrated to produce control signal for the autoswitching circuitry.

Method Used In PLL Based Descramblers



In most of the FilmNet descramblers, the field pulse was separated from the composite synch signal. This pulse train of field pulses is fed to an integrator. The inverter on the output of the integrator will only change state when the capacitor is sufficiently charged. The inverter output is high when there is no composite synch signal. The basic circuit given in the diagram could be adapted for most designs.

There are other methods for implementing autoswitching. These generally involve detecting the absence of the horizontal synch or detecting the inverted synch. The overall circuits used in these operations can be complex.

Detecting the absence of the horizontal synch is perhaps one of the simpler operations. The circuit used can be a straight comparator circuit as shown elsewhere in this chapter. The output of the comparator will be a clean synch train in the case of clear video.

The alternate field inversion used by FilmNet made autoswitching easy to implement. Since the inversion was on a field basis, the switching waveform for controlling the video polarity selection was a 25 Hz square wave. The high section of the square wave was used to select inverted video. This square wave was also used in the descrambler to identify the scrambled signal. In the case of a straight synch suppressed signal with no inversion, there was no square wave. The absence of the square wave indicated to the descrambler that video signal was clear rather than scrambled.

Implementing autoswitching with LuxCrypt descramblers is also straightforward. Since there would be no horizontal or vertical synch, this could act as a trigger. Since many of the descramblers designed for this system use PLLs, the second trigger would be a locked PLL.

Phase Locked Loops

The circuits given in the PLL diagrams are representative of some of the circuits used in descramblers. The 4046 is one of the most easily obtainable PLL ICs. It has been used extensively in non- commercial applications. Some of these designs were FilmNet and ORION decoders where the PLL ran at 15625 Hz to regenerate a line synch signal.

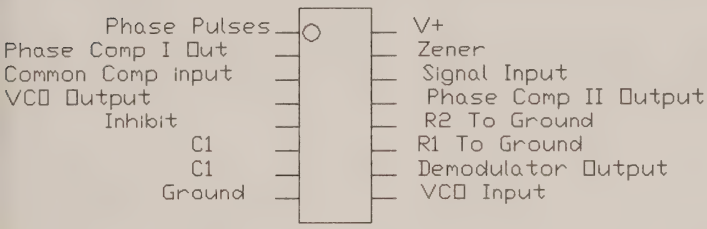
The main use of phase locked loops in descramblers is in the process of synch regeneration. It is not the intention of this chapter to teach the rudiments of phase locked loops to the reader. One of the best explanations of the operation and design of PLLs can be found on pages 428 to 437 of The Art Of Electronics by Horowitz and Hill.

In order to use a phase locked loop there must be some reference signal. This is generally a straightforward process if some reference signal such as the composite synch signal transmitted on FilmNet is present. Alternatively the suppressed horizontal synchs can be used. These would need to be sampled in order to be of use.

In descramblers, the commonest form of phase locked loop is one that runs at a multiple of the input or reference frequency. In the FilmNet signal, a signal must be derived to pull down the horizontal synch section to its correct level. Using a PLL running at 15625 Hz does limit the designer to using monostables to generate pulses such as those required for polarity testing. A PLL that uses a low frequency input to generate a high frequency output is commonly known as a frequency multiplier type. The PLL based FilmNet descrambler shown later in this chapter is a good example of this type of PLL.

In the PLL based FilmNet descrambler, the 2.0 MHz running frequency is divided down using combinational logic. The combinational logic provides a pulse of the correct duration for the synch pulldown. It also can be used to derive other signals such as a sample gate pulse or a polarity test pulse.

The 4046 Phase Locked Loop



The frequency range for the VCO is set by the equations shown below.

Fmin= 1/(R2*(C1+32pF)) When VCO control voltage = 0V = Vss
Fmax= Fmin + (1/(R1*(C1+32pF))) When VCO control voltage =Vdd

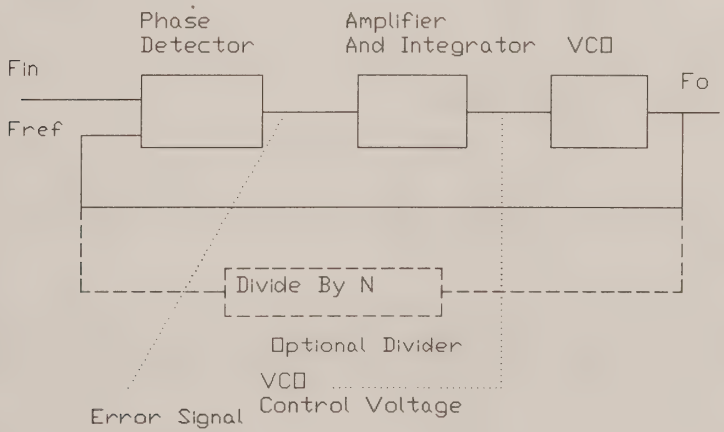
A low pass filter connected between pins 2 and 9 determines the lock range of the PLL. The capacitor is connected between ground and pin 9. The resistor is connected between pin 2 and pin 9. The lock range is derived from the equation below.

Fl=(Fmax-Fmin)/2

The capture range Fc is defined by the equation below.

Fc=((1/Pi)*(sqr((2*Pi*Fl)/(R3*C2)))).
R3 is connected between pins 2 and 9. C2 is connected between pin 9 and ground.

A Basic PLL As Used In Descramblers



Case Study: PLL Based FilmNet Descrambler

FilmNet has switched from SATPAC to D2-MAC EuroCrypt-M. The reason that this circuit is incorporated in version 4 is that it is a good example of what can be achieved with a purely analogue approach as opposed to using a microcontroller.

This FilmNet descrambler uses a 2 MHz phase lock loop to provide the horizontal blanking. Autoswitching is included though no provision for polarity detection is made. The circuit uses commonly available parts.

This circuit is for the main part the Hi Tech XtraVision FilmNet descrambler. It is reproduced here courtesy of Hi Tech.

The Composite Sync Demodulator

The FilmNet system transmits a composite synch signal on a subcarrier at 7.56 MHz. The descrambling of the FilmNet signal involves the demodulation of this carrier and using it to reinsert the synch levels in the picture.

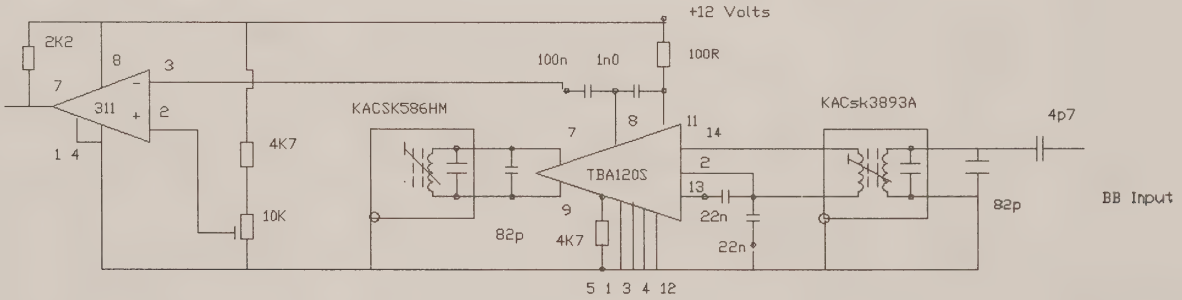
The demodulator is based on the TBA120S quadrature demodulator IC. Two off the shelf 10.7 MHz transformers are used to make the set up simple. These transformers are made resonant at the correct frequency by the addition of capacitors in parallel with the internal capacitors. The use of NP0 capacitors is essential in this application.

With the values given, the output of the composite synch is approximately 1V0 peak. This composite synch signal is fed to a 311 comparator which produces a negative going synch output. This signal is fed to the main logic section.

The Logic Section

The first part of the logic section is a phase adjustment. This is used to properly position the horizontal blanking window relative to the video.

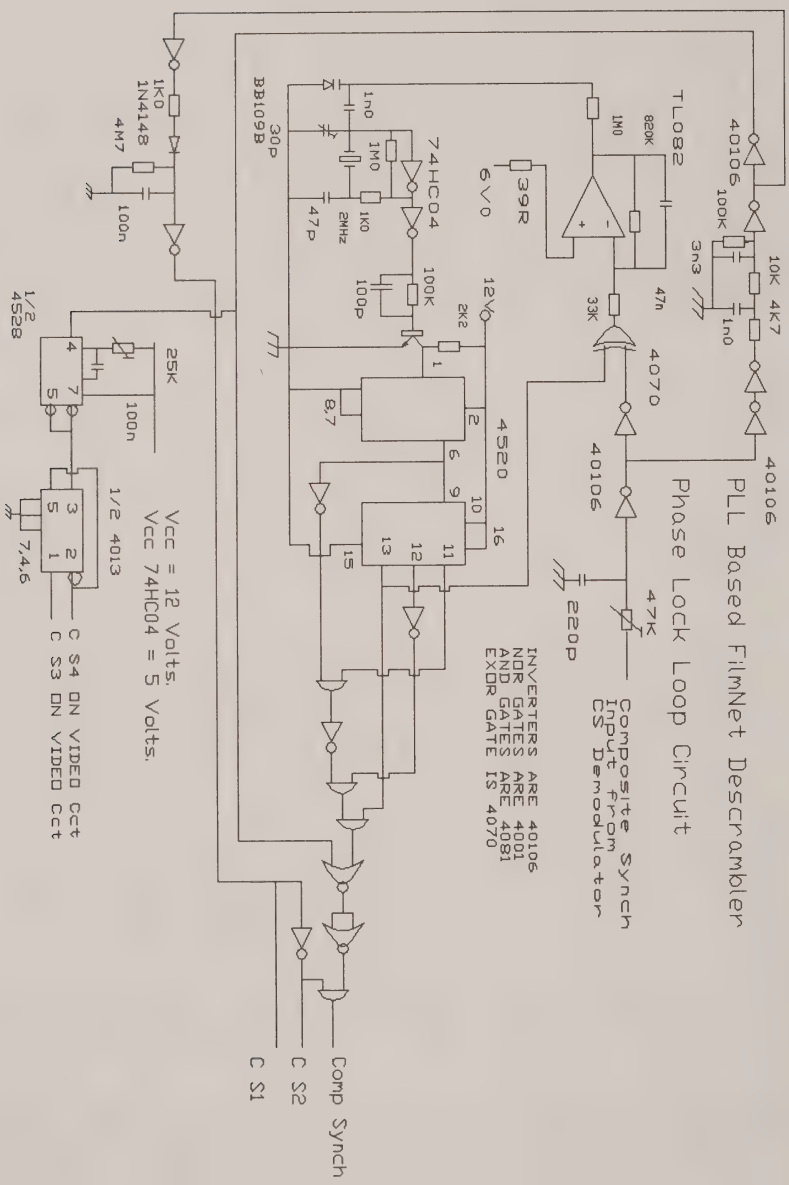
The inverters are 40106 Schmitt types. The phase detector is a 4070 EXOR gate followed by an integrator. The output of the integrator is the error voltage and is used to control the frequency of the VCXO.



Composite Sync Demodulator For PLL Based FilmNet Descrambler.

Input to 311 comparator

Output of 311 comparator


PLL Based FilmNet Descrambler
Phase Lock Loop Circuit
40106
10K 4K7
100K
1n0
3n3
TL082
820K
1M0
47n
33K
4070
40106
47K
220p
Composite Synch Input from CS Demodulator
39R
6V0
12V0
2K2
4520
16
10
9
6
2
1
8,7
15
13
12
11
74HC04
100K
100P
1n0
1M0
1K0
2MHz
47P
30P
BB109B
1K0
1N4148
4M7
100n
1/2 4528
25K
100n
1/2 4013
7,4,6
Vcc = 12 Volts.
Vcc 74HC04 = 5 Volts.
INVERTERS ARE 40106
NOR GATES ARE 4001
AND GATES ARE 4081
EXOR GATE IS 4070
C S4 ON VIDEO cct
C S3 ON VIDEO cct
Comp Synch
C S2
C S1

The VCXO is based on the 74HC04 inverter IC. This IC requires a supply of 5V0 to operate correctly. Its primary advantage is its low current operation. The output of the VCXO is converted to a 12V pk to pk signal by the transistor buffer.

The buffered 2 MHz signal from the VCXO is fed to the 4520 dual binary counter. This IC is used to divide the 2 MHz frequency. The use of combinational logic on the outputs produces a properly timed horizontal blanking window. This horizontal blanking signal is combined with the output of the field pulse separator, (integrator), to provide a properly timed composite blanking signal. This signal is used to control the synch insertion section of the video strip. An AND gate ensures that there is no synch signal when the descrambler circuitry is disabled by the autoswitching circuit.

The autoswitching circuit integrates the field pulses. If the receiver is not tuned to FilmNet, there is no field pulse present at the input to this circuit. This will cause S1 to close and S2 to open. This action passes normal polarity video to the video clamping and output stage. The output of the composite blanking AND gate is forced low by this circuit.

The Video Strip

The NE592 is used to provide a variable gain amplifier. The positive and negative outputs are fed to a number of 4066 switches. The first two switches, S1 and S2, control the selection of the video.

Control S1	S2	
0	1	Normal Video, Descrambler Off
1	0	Descrambler Active

The control signal for S2 could be used to effect loopthrough on some of the ASTRA receivers.

The second set of switches, S2 and S3, are the field polarity selectors. These are controlled by the outputs of the field polarity flipflop in the logic section. A preset is included so that any DC offset between the outputs can be nulled.

The selected video source is fed to a clamp to remove the dispersal waveform. The synch pull down is effected by turning on and off a transistor switch. The level of pull down is controlled by the 47K preset.

PLL Based FilmNet Descrambler - Video Strip
Vcc
VIDEO IN
75R
100u
10u
4K7
10K
10K
NE592
10K
14
10
1
12
3
8
5
7
S1 C TO C1 DIAG 2
S2 C TO C2 DIAG 2
S3 C TO C3 DIAG 2
S4 C TO C4 DIAG 2
S1
S2
S3
S4
C
I
100n
1N914
6V2
2K2
100R
15K
470R
100u
Video Output
150R
3K3
47K
4K7
COMP SYNCH INPUT - DIAG 2
S1 to S4 = 4066

Case Study: SAVE Descrambler

Though the SAVE system has largely fallen into disuse in Europe, it is still used on some cablenets and on Wire TV via satellite. It is a rather primitive if somewhat effective system. In the few months before the book went to print, there was a rumour that Red Hot Television, the hard core porn channel, would start to transmit again but this time would use SAVE. Everyone is still waiting.

This particular version of the SAVE descrambler is the standard hacker version. The design has been published in the Pink and Brown Book and the American electronic magazine "Radio Electronics".

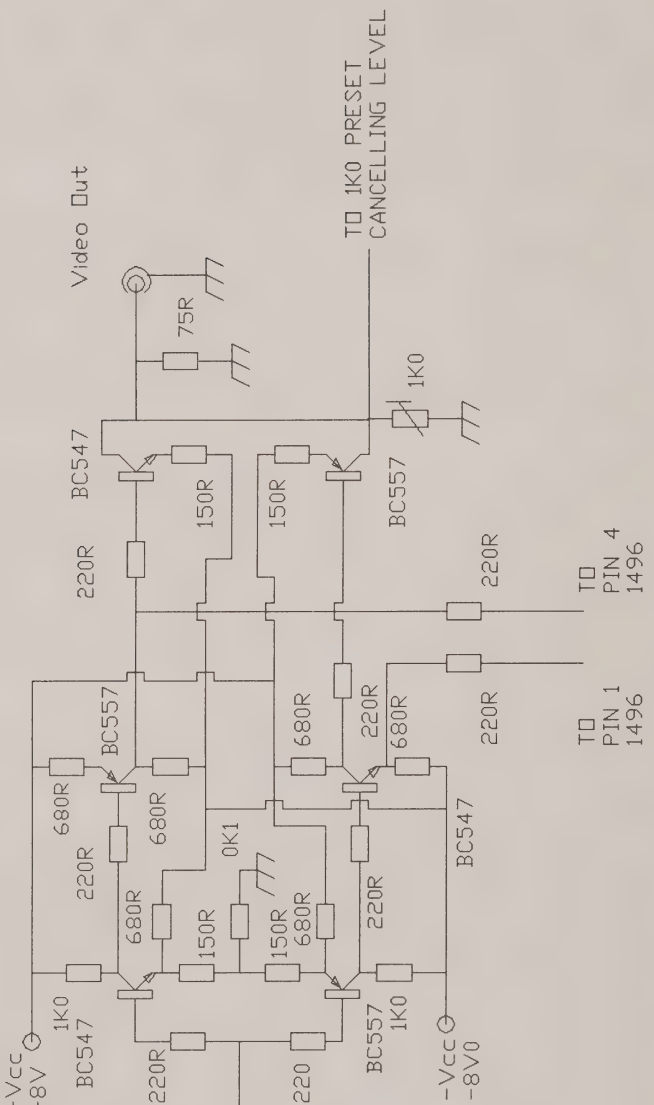
The video section is a Class B amplifier and is essentially the easiest part to set up. The input to this section must be unclamped. The level of the canceling sinewave is set by a front panel mounted potentiometer. The video level is set by the preset.

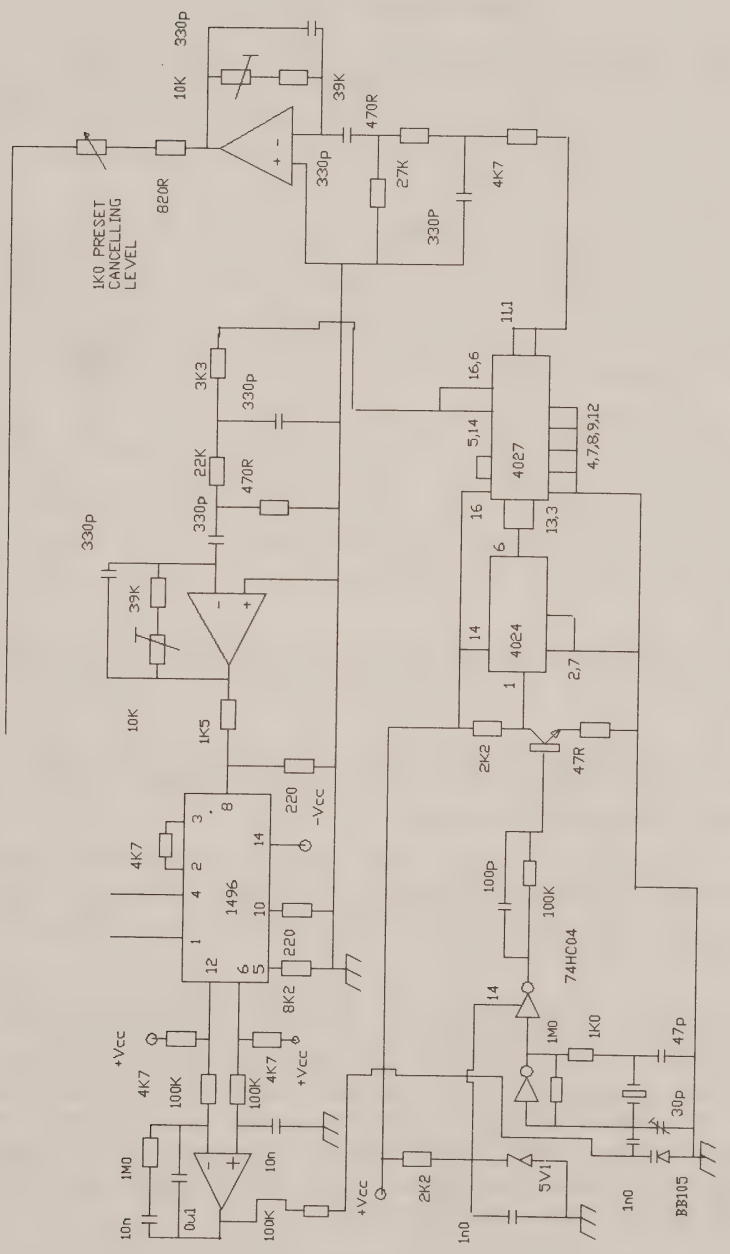
The phase lock loop section uses the 1496 balanced mixer as the phase detector. The voltage controlled crystal oscillator runs at a nominal 6.0 MHz. The actual frequencies used are slightly above or below 6.0 MHz. This frequency is divided by 16 in the 4024. The 4027 then divides this signal by 4 to give a nominal 94 KHz. The outputs of the 4027 are 90° out of phase. This is to compensate for the phase shift in the phase lock loop. The 10K presets in the elliptical filters are set for best response.

The disadvantage of the design is that it needs a number of crystals to cope with a multiple carrier version of the SAVE descrambler which was developed by SAT-TEL.

The most recent widespread use of the SAVE system was as the initial scrambling system for the Red Hot Television channel. The problem was that a very bad choice of crystal frequency was made. It was 6.144 MHz, an off-the-shelf crystal frequency. As a result there was no real problem in hacking it.

SAVE Descrambler Video Section




SAVE PLL Section
1K0 PRESET CANCELLING LEVEL
820R
10K
330p
39K
470R
330p
27K
330P
4K7
3K3
330p
22K
470R
330p
39K
10K
1K5
220
-Vcc
4K7
1496
220
8K2
+Vcc
4K7
100K
100K
4K7
+Vcc
1M0
10n
0u1
10n
100K
+Vcc
2K2
5V1
1n0
1n0
BB105
1U1
16,6
5,14
4027
4,7,8,9,12
16
13,3
6
4024
14
1
2,7
2K2
47R
100p
100K
74HC04
14
1M0
1K0
47p
30p

Case Study: LuxCrypt

The IRDETO system was patented in 1982. It was the forerunner of the OAK ORION system. From studying the patent, it would appear that the most daunting aspect of the system is the digital audio. The scrambling system used by RTL4-V is known as LuxCrypt and is a subset of the IRDETO system.

The basic strength of the system is that it relies on the replacement of synch pulses to scramble the video. Since there are no synch pulses in the scrambled video signal, the television receiver cannot lock the picture. The old synch generator descramblers such as the Digisync and the PDS Synch Generator could lock the scrambled IRDETO signal in its present format.

The main strength of the LuxCrypt subset is the active video inversion. A number of types of video inversion are allowed for in the specification. The type used in the January 1990 upgrade was Average Peak Level, (pronounced apple). This type of inversion inverts the video polarity if the amount of white or black in a scene exceeds a preset threshold. The shortest time between inversions is three seconds.

Many of the present pirate descramblers on the market detect the polarity of the video at the start of each field. This is not the best method.

There is a polarity key in each line. Some pirates disagree with this view claiming that the polarity key is actually an artifact or glitch left over from the scrambling process.

From observation, it appears that it is a polarity key. The official descrambler is a low cost unit and as such it would need some facility for re-establishing the black level in the scrambled video. This polarity bit would provide such a facility.

The colour burst does not change in time relative to the other components in the video signal. It is therefore a usable reference. The basic idea is to detect the colour burst using a tuned circuit and use it to synch a phase locked loop such as the 4046 or the TBA920. The SRP1000 design (FilmNet descrambler in version 3) could probably be adapted for use by using a peak detector or comparator on the output of the tuned circuit. The output of the tuned circuit reaches its maximum at the end of the colour burst.

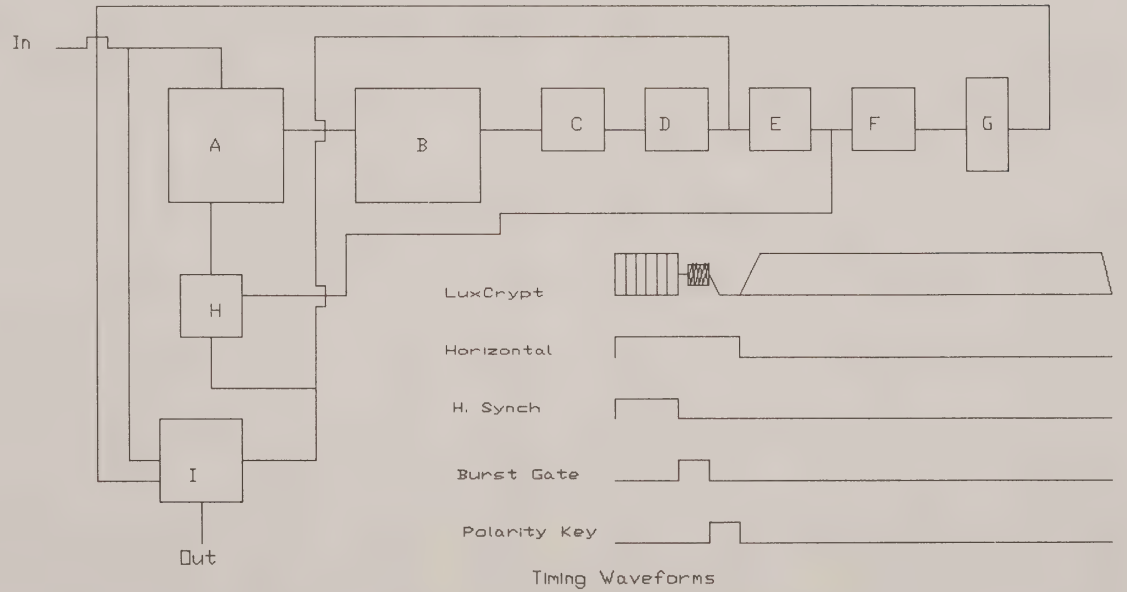
Colour Burst Detector Circuit

This circuit can be used to detect the colour burst in an RTL4V Luxcrypt descrambler. The burst gate is necessary to prevent triggering on chrominance information.

To adapt this circuit to detect the 4.0 MHz data burst, replace the marked 330pF capacitor with a 390pF capacitor in parallel with a 15pF trimmer.

An Experimental LuxCrypt Descrambler

A: Colour Burst Detector. B,C,D: Line Synch Regen. (page 3-30)
E,F: Monostables (page 3-2) G: Polarity Key Detector (page 3-18)
H: Field Monostable (Triggered If No Burst Is Present)
I: Synch Insertion Multiplexer (page 3-6)



Timing Waveforms

The field synch can be recreated by counting the number of colour bursts and triggering a set of monostables. The first monostable would be used to position the field pulse.

The procedure for determining the video polarity can be broken into three steps.

1. The Colour burst is detected and used as the timing reference.

2. The Burst, (Blanking level), is sampled.

3. The polarity key is sampled.

If the burst level is higher than the polarity key level then the video polarity is normal.

If the burst level is lower than the polarity key then the video polarity is inverse.

If the burst level is equal to the polarity key then the signal is not scrambled.

The 2 MHz PLL used in the PLL FilmNet design could be adapted for use in this application. The main change would be in the horizontal blanking decoding on the output of the counter. A comparator would be used to detect the colour burst peak. A sampling gate circuit such as that used in the SRP1000 design would eliminate some of the false triggering.

On Astra 1-C, RTL-5 is now using what appears to be a version of the LuxCrypt system. Some of the old pirate descramblers will not lock up on the signal, perhaps indicating that the system may be employing APL inversion.

Hi-Tech Galaxy RTL4V Stand Alone Descrambler

This is a stand alone descrambler for the LuxCrypt system as used on the RTL-4 Veronique channel. The system as implemented on Luxcrypt is a minimal system. It is a derivative of the IRDETO system. The audio scrambling facility, IRDETO's most powerful aspect, not used.

The main attraction of RTL-4V is that many of the terrestrial television sit-coms and serials are shown. Unfortunately, they are scrambled as RTL4-V only buys the local rights. The Luxcrypt system is a token scrambling system in that it is not really meant to offer any serious protection.

The stand alone RTL4-V descrambler is a PLL based design. It is essentially three sections; the video input strip, the PLL and the video output strip.

The Video Input Strip

The first part of the video input strip uses two discrete transistor amplifiers to amplify the baseband input. The input level of the second amplifier is controlled by a 500R preset on the output of the first amplifier.

The second amplifier feeds a video bandpass filter. The output of the filter is buffered and fed to an inverting and non inverting buffer. These provide the necessary normal and inverted video signals necessary for descrambling the signal.

The PLL

The VCXO of the phase locked loop is constructed around a 5.752 MHz crystal. Two gates of a 74HC04 hex Schmitt inverter are used. The phase comparator is a switched type. The switch is a 4066 gate and this switches between the oscillator output, CLK5M7, and the sampled clock signal.

The horizontal and vertical timing are generated by different sections of logic. The field timing is used to trigger the horizontal timing section constructed around the 27256 EPROM and also to trigger the decoder select control.

The core of the descrambler is the 27256 EPROM. The PLL clocks two counters which control the addressing on the EPROM. By using a series of counters and combinational logic on the EPROM outputs, it is possible to generate the sample and control slots necessary to descramble the signal. This is an elegant solution to the problem.

The Video Output Strip

The video output stage owes much to the Oak ORION design published in the Pink And Brown book. It uses 4066 switches to effect the clock sampling and the clamping.

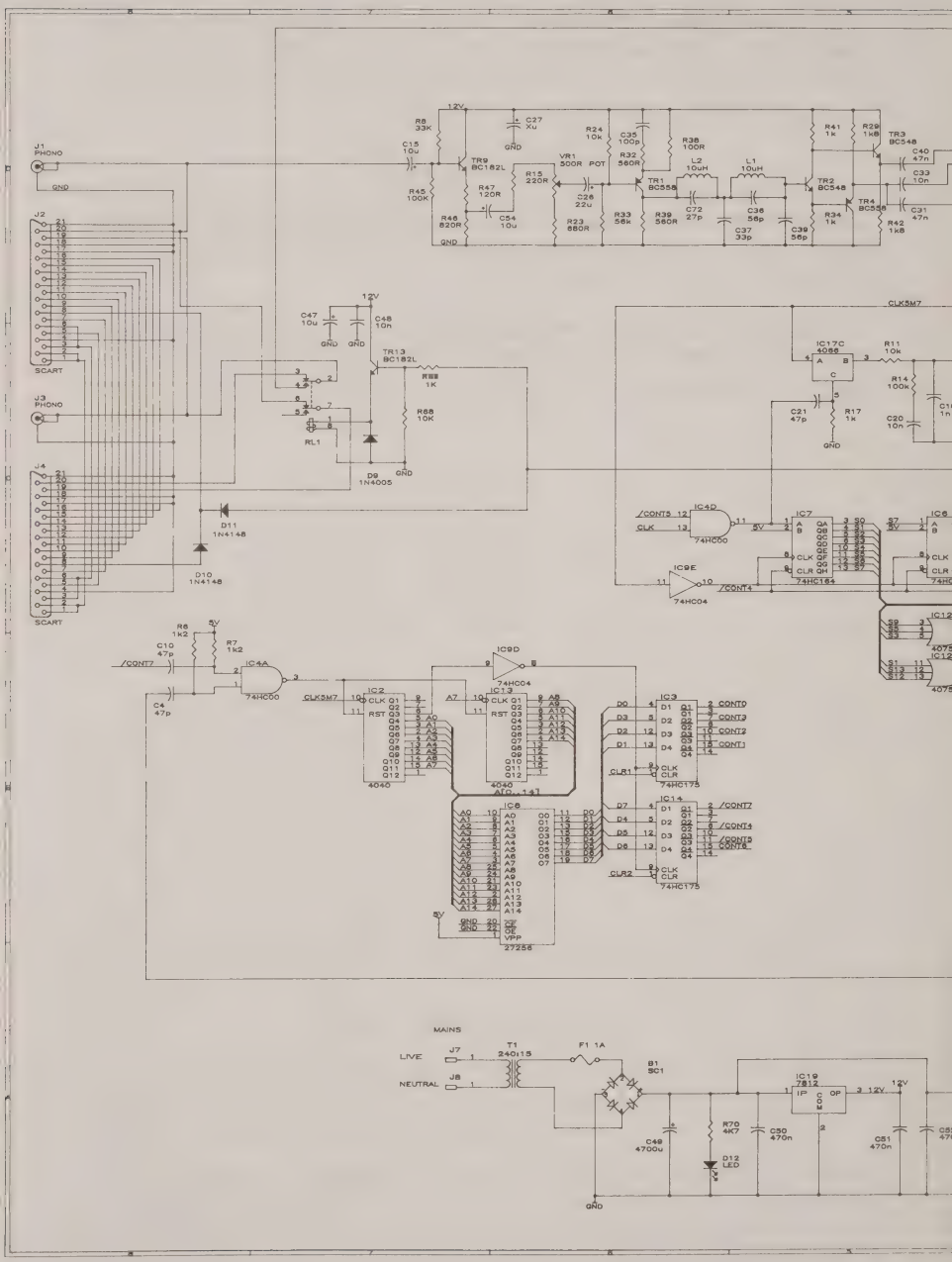
The clamping is necessary to restore the synch pulses and blanking in the descrambled video. The main switching for this operation is performed by a 4051. The video output is buffered and then fed to the output.

The connectors on this descrambler are the same as those on the other Galaxy type descramblers, two SCART connectors and two phono connectors. The loopthrough and switching is controlled by the PLL logic. A relay is also used in this design.

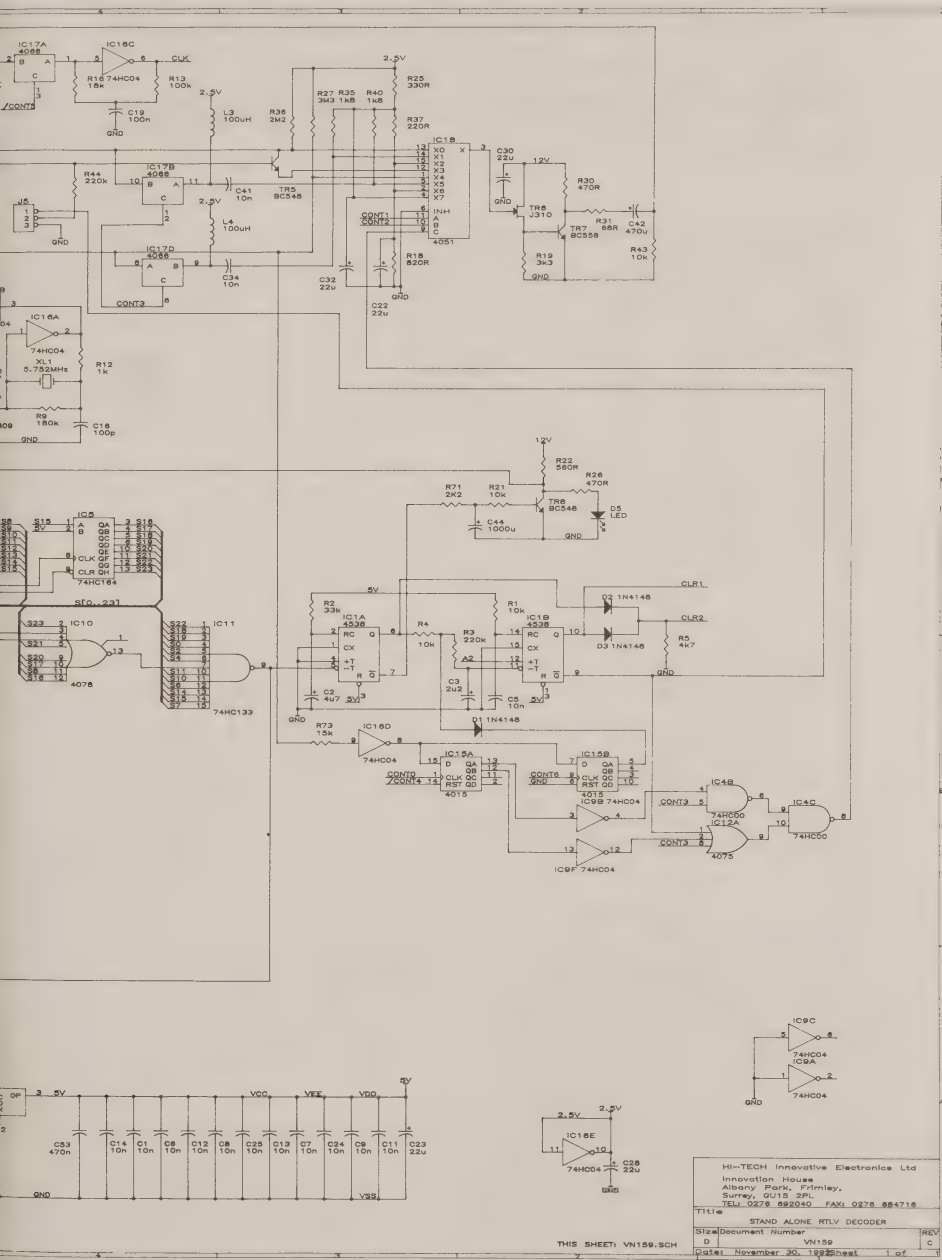
The Power Supply

The power supply uses a 15 Volt transformer feeding a bridge rectifier. A 1 Amp fuse is included prior to the bridge rectifier. An LED indicates that power is present.

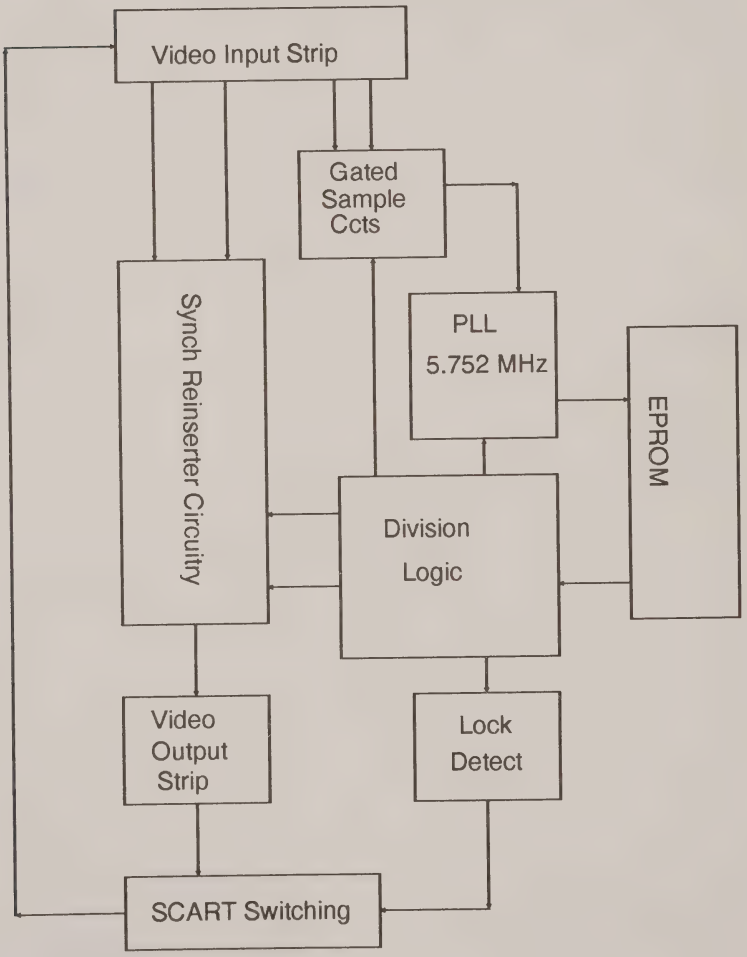
Two IC regulators are used to produce the +12 Volts and +6 Volts supply lines. Each has its own reservoir capacitor and separate decoupling capacitors.



3: Descrambler Building Blocks



RTL4-V Descrambler Block Diagram



Case Study:The "Radio Plans" Design

This is the circuit that was published in the "Radio Plans" magazine. The magazine issue was seized by the courts. A French newspaper, "Le Quotidien", then published the controversial design. In that way the design reached more people than it ever would have. It also became public knowledge.

The "Radio Plans" descrambler was designed for use on a SECAM signal rather than a PAL signal. The timing on the PAL version is slightly different. In terms of commercial hacking the "Radio Plans" descrambler is not viable. Most of the subsequent hacker circuits replaced major sections of the circuit with simpler more repeatable circuitry. The resulting descrambler was cheaper and overcame the chip shortage problem that occurred.

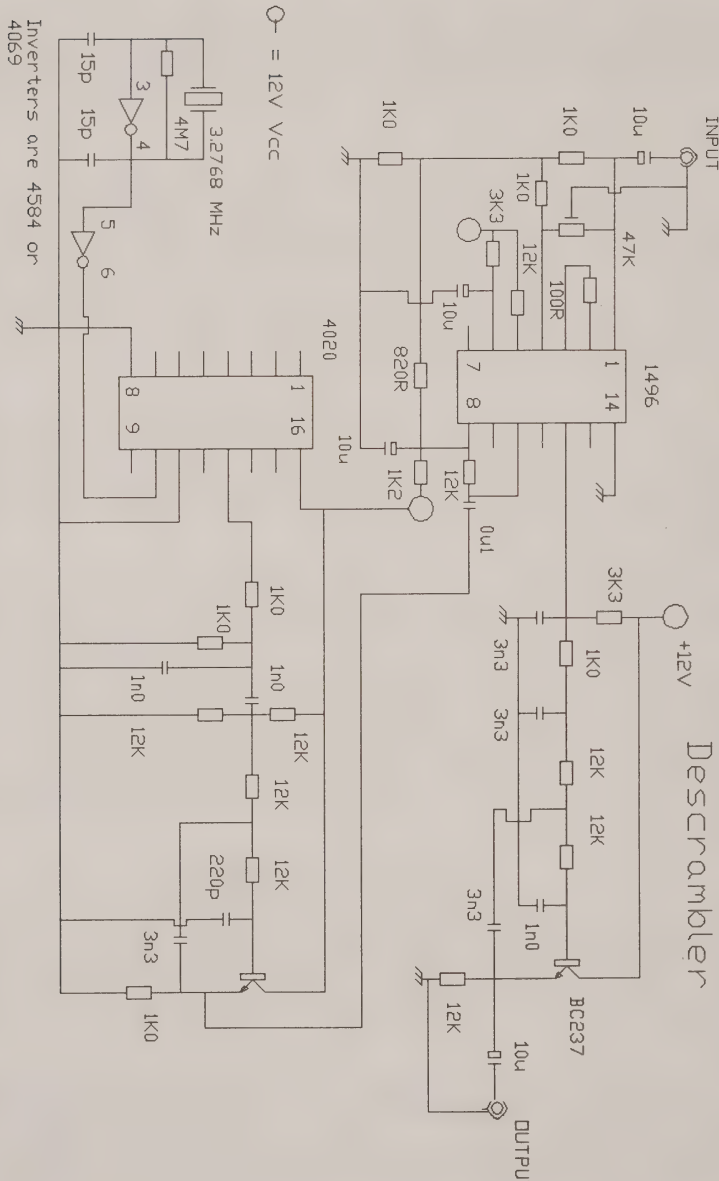
The versions of Discret currently in operation have, in the majority of cases, been upgraded to counter this particular design. It is highly illegal to use a pirate descrambler in France. It is also illegal to use a pirate cable descrambler in Ireland. The following case study is for informational use only.

The Radio Plans circuit can be considered as five sections; the audio descrambler, the start of video detector; the video descrambler; the video multiplexing section and the synch generator circuit. The design used a number of rather expensive integrated circuits. It was exceedingly popular with the home constructors. The shops selling the kits had to reorder by the components by the hundred. This massive demand led to a shortage of the critical ICs. Hackers were forced to improvise and adapt other circuits. Some of these adapted circuits are shown later.

The Audio Descrambler

The audio in the Discret system is rotated about a 12.8 KHz carrier. The "Radio Plans" design uses a crystal oscillator running at 3.2768 MHz. The oscillator is based on two 4584 CMOS inverters. One inverter is used as the oscillator and the other inverter is used as the buffer.

The output of the oscillator is fed to a 4020 divider. This divides the oscillator frequency by 256 to produce the 12.8 KHz carrier. The output of the 4020 is fed to a transistor filter. This is used to filter the harmonics present and to convert the square wave to a sine wave.


Radio Plans Discret Audio
Descrambler
INPUT
10u
1K0
47K
1K0
3K3
12K
100R
10u
1496
820R
1K2
12K
0u1
+12V
3K3
1K0
12K
12K
3n3
3n3
1n0
BC237
12K
10u
OUTPUT
4020
1K0
1K0
1n0
1n0
12K
12K
12K
12K
220p
3n3
1K0
= 12V Vcc
3.2768 MHz
4M7
15p
15p
Inverters are 4584 or 4069

The 12.8 KHz sine wave is then fed to a 1496 balanced demodulator IC. The 1496 circuit is configured for single rail operation. The scrambled audio is also inputted to this IC. A 47K preset provides balancing and cancellation control.

The output of the 1496 is fed to a single transistor filter to remove any remaining 12.8 KHz signal from the descrambled audio. The descrambled audio is then fed back to the SCART connector.

The Start Of Video Detector

The scrambled video from the output of the first TBA970 on the video descrambler section is fed to a transistor two stage low pass filter. This filter removes the chrominance from the video waveform. The resulting video signal is then amplified by a factor of five. The signal from the op-amp is fed to the back level sample and hold and to the comparator.

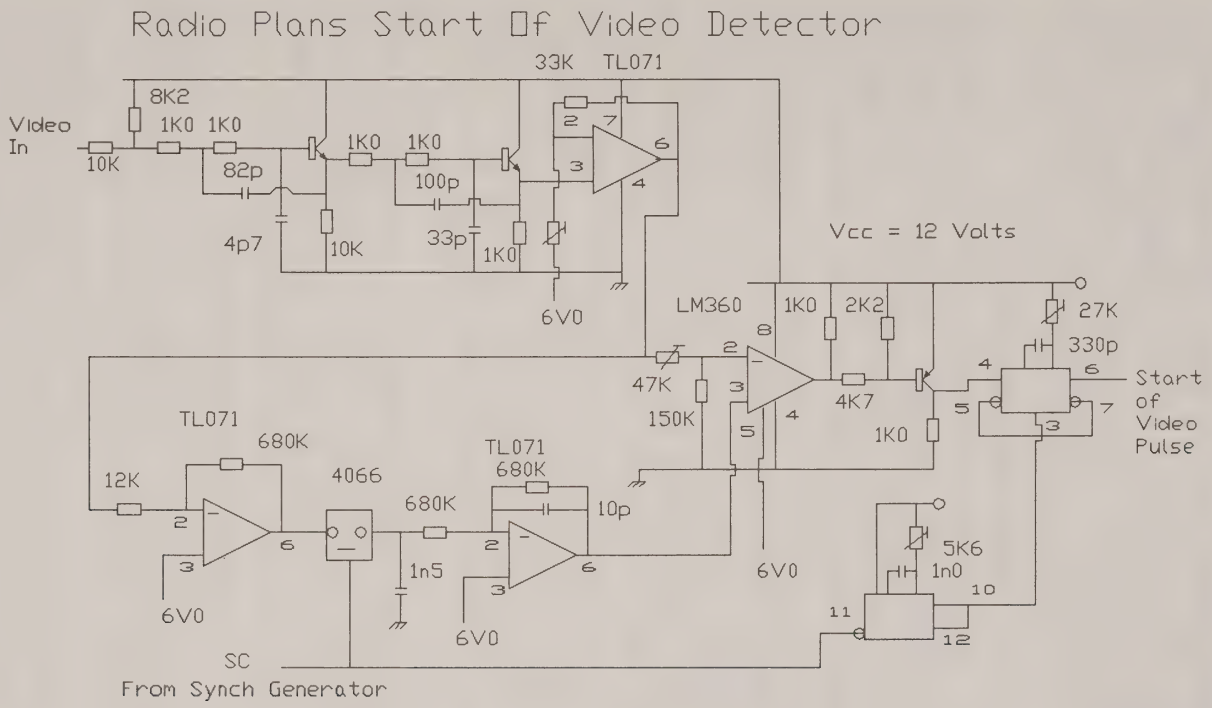
The sample and hold circuit is based on a 4066 as the sampling switch and a polystyrene 1n5 capacitor as the storage or hold capacitor. The op-amp used as the buffer is a simple TL072 type. In this application it is configured as a non inverting amplifier with unity gain. The output of the amplifier is fed to the comparator.

The comparator is continually comparing the voltage difference between the sampled black level and the video signal. It has to detect a rise of approximately 150 mV. The sample gate is controlled by the sandcastle pulse generated by the synch generator circuit. The output of the comparator is fed to a transistor level converter. This converts the comparator output to CMOS logic levels. It is not strictly required.

The sandcastle pulse also triggers the first monostable. This generates a delay to position the start of video window in the correct area of the line. The output of this monostable controls the enabling of the start of video pulse monostable. This second monostable generates a fixed length pulse to indicate the start of video.

The Video Descrambler

The video descrambler section is composed of delay lines and black level clampers and amplifiers. The delay lines used are the TDA4560. These are configured to give an 888 nS delay on the video. The TDA4560 gyrator delay line has a good response as far as 5 MHz. The gyrator delay line has a loss of 6 db. This means that some amplification is required to restore the level to normal. The signal must also have black level clamping. This is essential for proper descram-


Radio Plans Start Of Video Detector
33K
TL071
8K2
1K0
1K0
Video In
10K
82p
4p7
10K
1K0
1K0
100p
33p
1K0
6V0
Vcc = 12 Volts
LM360
1K0
2K2
27K
330p
47K
150K
4K7
1K0
Start of Video Pulse
TL071
680K
12K
4066
680K
TL071
680K
10p
1n5
6V0
6V0
6V0
5K6
1n0
SC
From Synch Generator

bling. If there is a difference in black levels between each of the delayed video signals, there will be strobing on the screen. This effect is similar to the effect on some FilmNet descramblers when the two fields are not at the same level.

There are four outputs from the video descrambler. Three, one from each TBA970, are fed to the video multiplexing circuitry. The output from the first TBA970 is also fed to the Start Of Video Detector circuit.

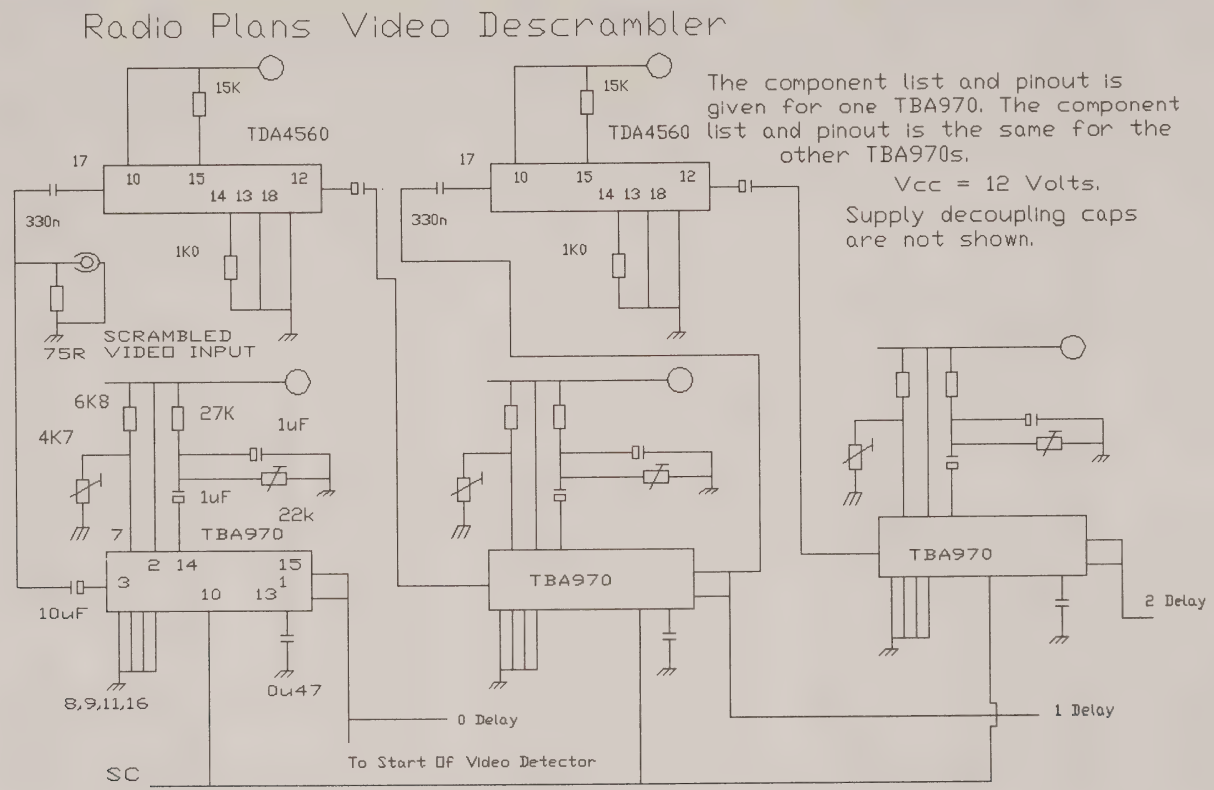
The Video Multiplexing Circuitry

There are basically four elements in this section. The first of these is the monostable timing chain. This is a chain of three monostables. The first monostable generates a delay that positions the outputs of the two other monostables. These other monostables generate the windows or Data signals for the flipflops.

The flipflops control the multiplexer. The D pin on each flipflop is only high during its respective window. This means it is only possible for the flipflop to change the state of its output during that window. The start of video pulse provides the clocking pulse (CL) on each flipflop. The LI signal form the synch generator circuit is fed to the RESET pin on each flipflop. This ensures that the multiplexers are switched to the two delay mode by resetting the flipflops at the start of the horizontal synch pulse. This is to ensure that the synch and colour burst section of the line pass through without being delayed. This is essential for proper line stability in the descrambled picture.

The multiplexer used is the 4053. This IC has three single pole double throw (SPDT) switches. Only two of the switches are actually used in this design. In some of the commercial pirate designs, a single 4066 with two inverters was used to replace the 4053.

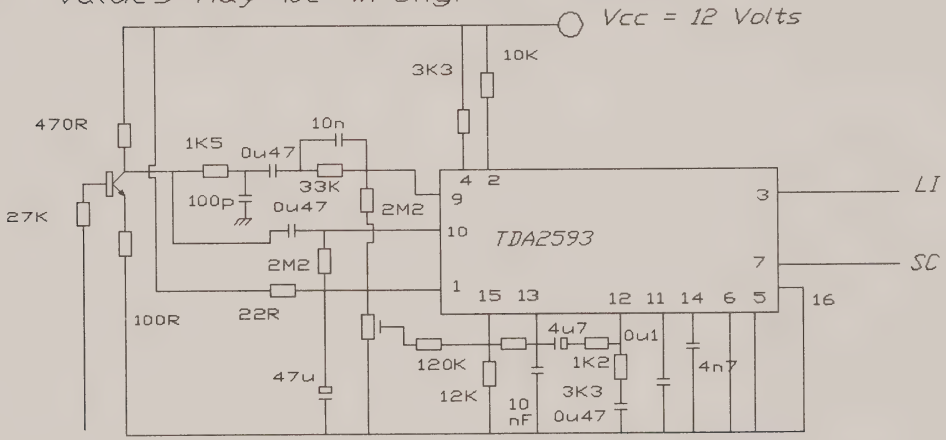
The output of the second multiplexer switch is fed to the video amplifier. This is the TDA1034 or LM318 operational amplifier. The output from the TDA1034 is taken to the push pull amplifier. The complete video amplifier section is replaced in most of the pirate designs by a single transistor emitter follower on the output of the second multiplexer switch.


Radio Plans Video Descrambler
15K
TDA4560
17
10
15
12
14 13 18
330n
1K0
SCRAMBLED
75R VIDEO INPUT
6K8
27K
1uF
4K7
1uF
22k
7
TBA970
2 14
15
3
10
13
1
10uF
8,9,11,16
0u47
0 Delay
To Start Of Video Detector
SC
1 Delay
2 Delay
The component list and pinout is given for one TBA970. The component list and pinout is the same for the other TBA970s.
Vcc = 12 Volts.
Supply decoupling caps are not shown.

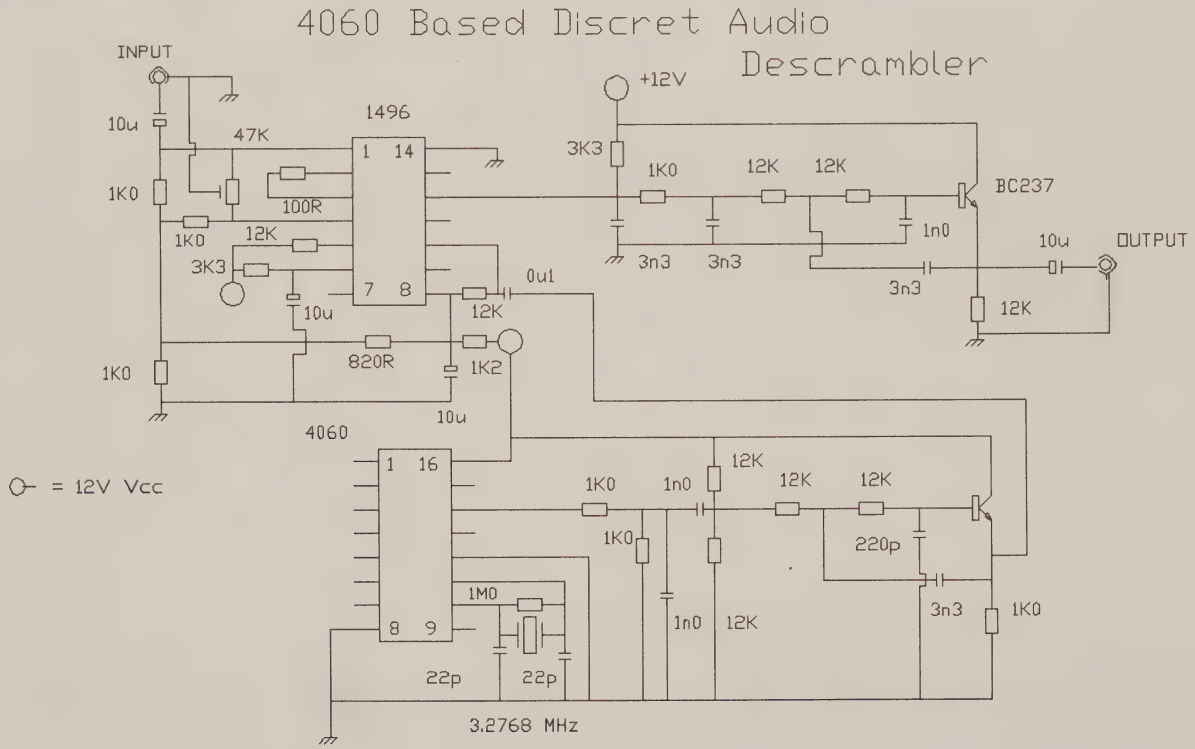
Radio Plans Video Multiplexing
Monostables Are 4098s.
Sandcastle Pulse From Synch Generator
Window Position
Window 1
Window 2
22K
470p
5K6
100p
5K6
100p
SoV
LI
15K
100R
1K2
1K2
10R
10R
3K3
3K3
1N4148
1N4148
LM318
10u
Video Output
Cx
Cy
Co
Bx 2
By1
Mux C
Part Of 4053
Mux B
0 Delay
1 Delay
2 Delay
To Video Descrambler Circuit
SDV = Start Of Video Pulse
LI = LI signal from Synch Generator
Pins 14,13,12,11,8,7,6 On the 4053 are grounded.

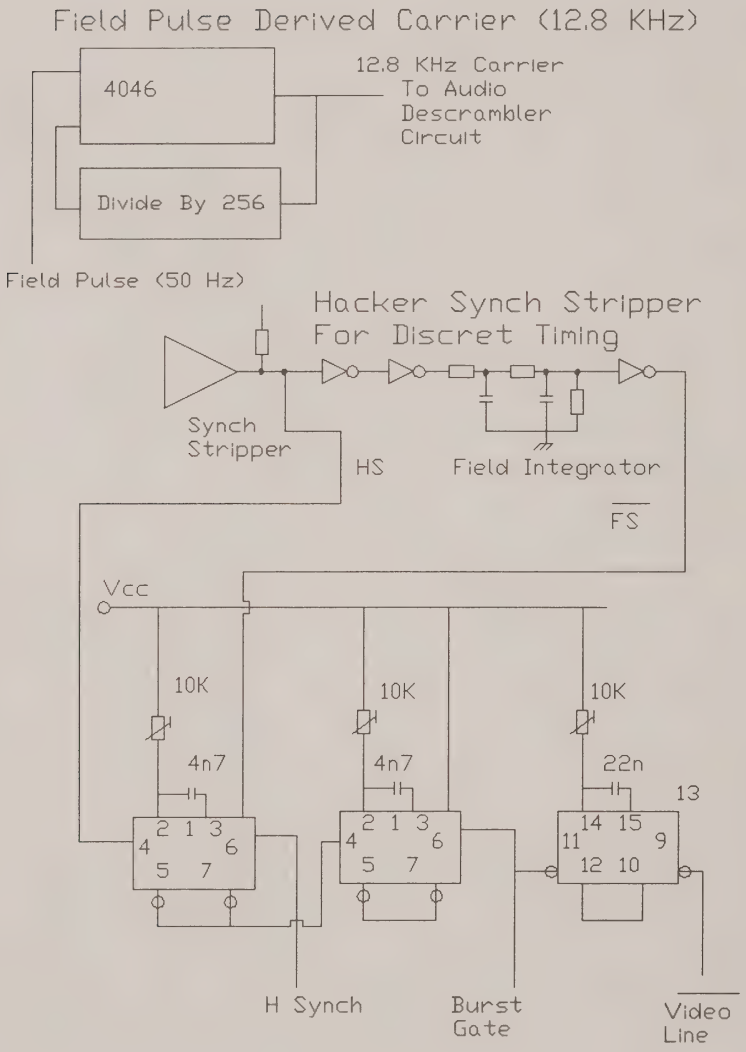
RP Synch Generator Circuit

Note: The photocopy of this circuit was not clear. Some of the connections and values may be wrong.



Signal from the output of first TBA970. (Video Signal)


4060 Based Discret Audio
Descrambler
INPUT
10u
47K
1K0
100R
1K0
12K
3K3
10u
1496
1 14
7 8
+12V
3K3
1K0
12K
12K
BC237
1n0
3n3
3n3
10u
OUTPUT
3n3
12K
0u1
12K
1K0
820R
1K2
10u
4060
1 16
8 9
1M0
22p
22p
3.2768 MHz
1K0
1n0
12K
12K
12K
1K0
1n0
12K
220p
3n3
1K0
= 12V Vcc



The comparator synch stripper circuit is given elsewhere in this chapter.

The Synch Generator

This section of the circuit is used to generate the sandcastle control signal and the LI control signal. It strips the synchs from the scrambled video and uses them to phase lock a line oscillator.

It is a standard television horizontal synch circuit but has proven to be too costly for anything other than home construction. This circuit has largely been replaced by a synch stripper and monostable combination.

The Hi-Tech Discret J Card

The Discret card is perhaps one of the best examples of what can be achieved with a microcontroller based design. It uses a 68705 EPROM type microcontroller as the microcontroller.

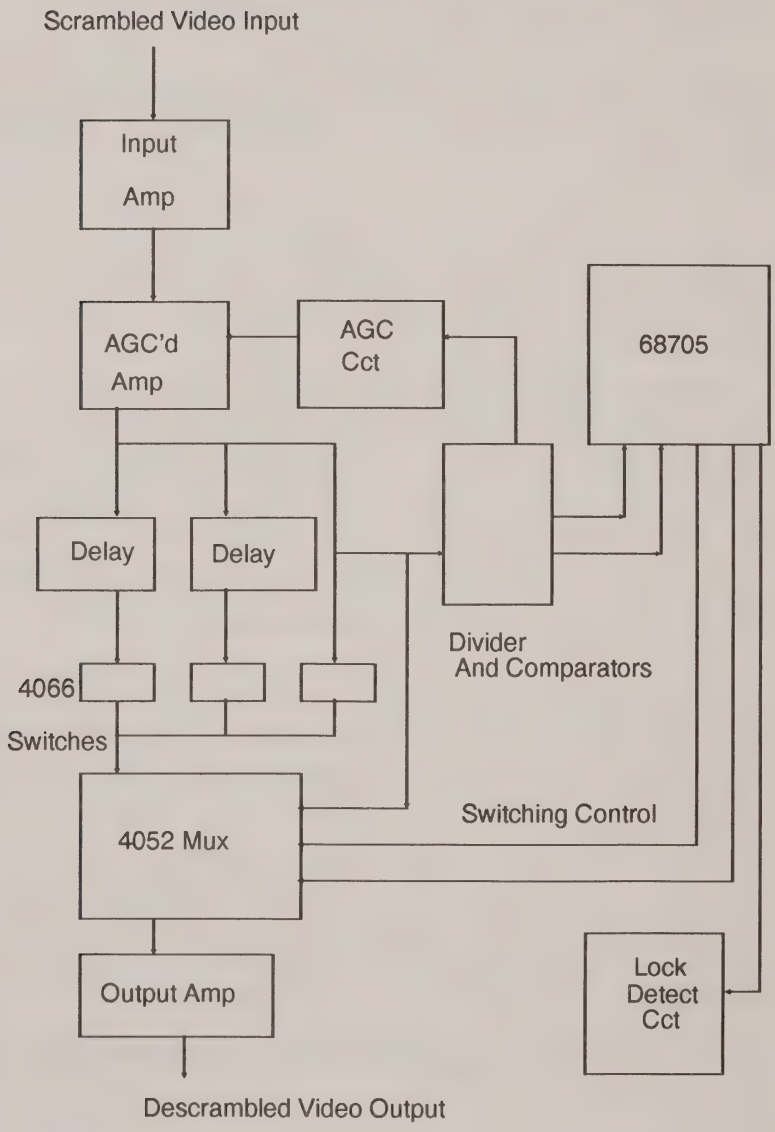
The Discret system operates by delaying the video in each line by one of three delays; 0 nS, 902 nS or 1804 nS. The standard method of descrambling the signal was pioneered by the Radio Plans design. The method involved detecting the rise from black level to the start of video. If the video was not delayed, the two delay units were added. If the video was delayed by one unit, then another delay unit was added. If the video was delayed by two units then it was gated straight through. This created a black band at the left hand side of the screen, but on most television it was lost on the overscan.

The problem with trying to detect the rise from black level was that it was wide open to countermeasure by the programme provider. To nuke the first Radio Plans based descramblers, all Canal Plus had to do was insert a level other than black in the delay area. The descramblers could not find the black level and hence their detection circuitry failed.

Hi-Tech has kept the video descrambling section and used a different method for slotting in the delays. The necessary data to descramble the signal is transmitted in one of the VBI lines. By using this information and processing it with the 68705, it is possible to set the delay slots without using the rise from black detection.

The descrambler can be considered in two sections, the video strip and the microcontroller section.

Hi-Tech Discret J Card



The Video Strip

The input section of the video strip is a two transistor design. A FET configured as a variable gain resistor provides automatic gain control. This is essential for the data and synch stripping. The AGC is applied to the input of the video amplifier. The output of this amplifier is buffered and fed to the delay lines.

Three video signals are necessary to descramble the signal; an undelayed video signal, a one delay video signal and a two delay video signal. In order to maintain a constant amplitude among the signals, two presets are included in the 0 delay and the 2 delay chains. A single terminating resistor is included on the 1 delay chain. The switching between the video signals is effected by three 4066 switches. The output of each of these switches is fed to one of the inputs on a 4052 multiplexer.

The 4052 controls the switching between synch and video signals. The descrambled video is fed to a two stage transistor buffer. The video output is taken from a 1K0 preset on the emitter of the second transistor.

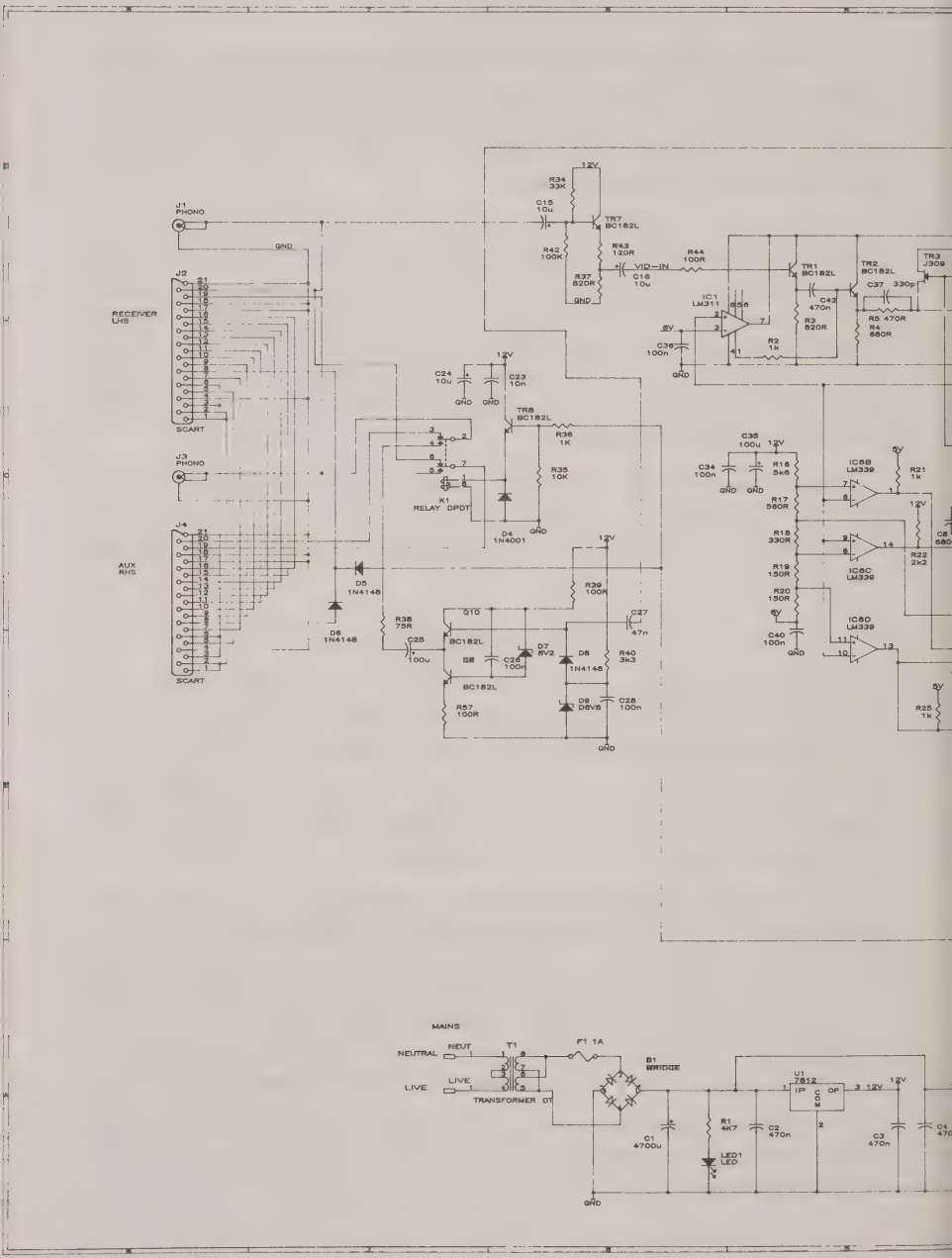
The Microcontroller Section

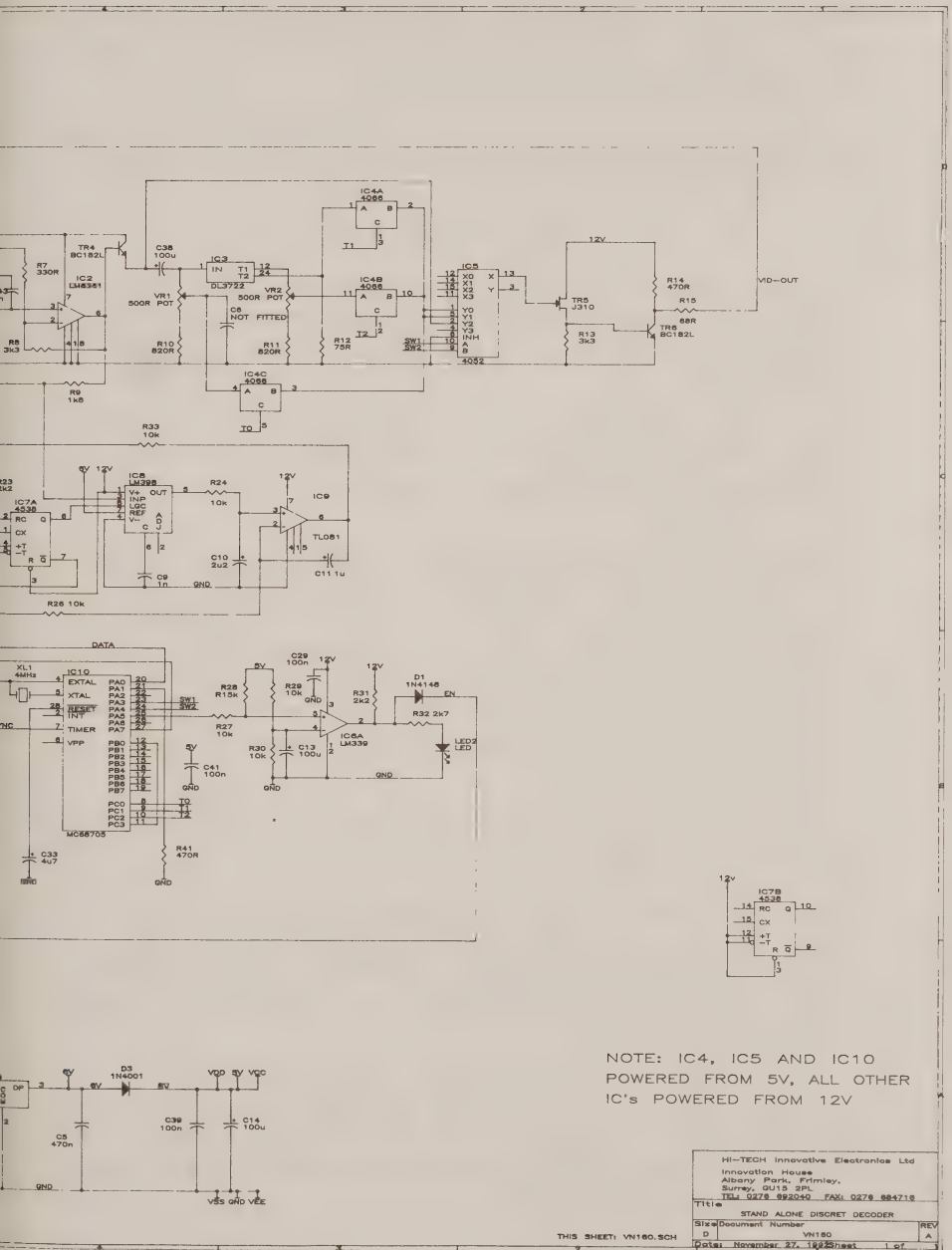
The microcontroller used in this design is the 68705. This is a secured EPROM version. Should an upgrade be necessary, Hi-Tech can easily issue a replacement. The crystal frequency is 4.0 MHz.

The control signals are extracted from the video by a divider and comparator network. The topmost comparator strips the data from the video signal. This is fed to the microcontroller.

The second comparator is the AGC comparator. This triggers the 4538 monostable. The monostable creates a 1 uS window in which to sample the blanking level. A gated comparator samples the signal and the output is integrated and fed to the TL081 AGC amplifier. In this way the amplitude of the video signal is kept constant. This is an essential requirement for this type of decoder as the divider - comparator chain will not operate properly if the voltages are off spec.

The third comparator is the synch stripper. This provides a synch train the the microcontroller so that the correct lines can be selected for data extraction.


J1 PHONO
GND
J2
RECEIVER LHS
SCART
J3 PHONO
J4
AUX RHS
SCART
12V
R34 33K
C15 10u
TR7 BC182L
R42 100K
R43 120R
R37 820R
GND
VID—IN
C16 10u
R44 100R
TR1 BC182L
TR2 BC182L
TR3 J309
C37 330p
IC1 LM311
8S6
C42 470n
R3 820R
R5 470R
R4 680R
8V
C36 100n
R2 1K
C24 10u
C23 10n
TR8 BC182L
R36 1K
R35 10K
K1 RELAY DPDT
D4 1N4001
C35 100u
C34 100n
R16 5k6
R17 560R
IC8B LM339
R21 1k
R18 330R
R19 150R
R20 150R
C40 100n
IC8C LM339
IC8D LM339
R22 2k2
D5 1N4148
D6 1N4148
R38 75R
Q10 BC182L
C25 100u
C26 100n
D7 8V2
D8 1N4148
R39 100R
C27 47n
R40 3k3
D9 D8V8
C28 100n
R57 100R
R25 1k
MAINS
NEUTRAL
LIVE
NEUT
LIVE
T1
TRANSFORMER DT
F1 1A
B1 BRIDGE
U9 7812
IP
OP
COM
C1 4700u
R1 4K7
LED1 LED
C2 470n
C3 470n
C4 470n



NOTE: IC4, IC5 AND IC10 POWERED FROM 5V, ALL OTHER IC's POWERED FROM 12V

Hi-TECH Innovative Electronics Ltd
Innovation House
Albany Park, Frimley,
Surrey, GU15 2PL
TEL: 0276 692040 FAX: 0276 684716

Title	STAND ALONE DISCRET DECODER	
Size: D	Document Number: VN160	REV: A
Date: November 27, 1992	Sheet 1 of 1	

THIS SHEET: VN160.SCH

The microcontroller will supply the switching control signals to the 4052 multiplexer. The switching control signals combines the proper synch signals with the descrambled video.

A lock detect circuit is operated by the microcontroller. This circuit will send a descrambler select signal to the SCART control circuitry.

EBU Resyncher

Some readers of previous versions have expressed an interest in receiving signals that have the synchs corrupted either intentionally, as is the case with EBU sound in synch, or accidentally as is the case with poor CNR.

In the past, descramblers like the PDS synch generator have been used to lock up these signals for display. While we do not have the circuit diagram of the PDS synch generator, we do have a somewhat cheaper alternative.

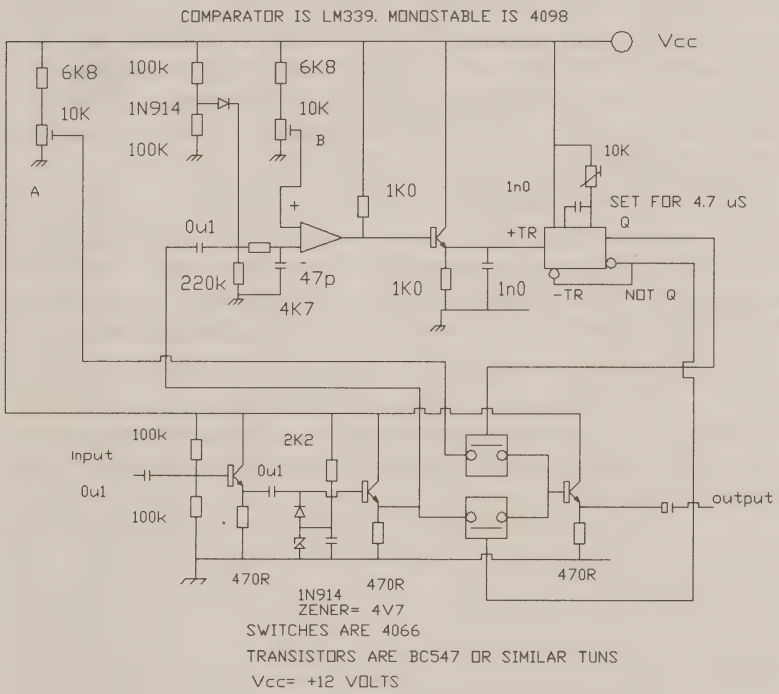
The EBU format system is designed to optimise the satellite power. On a normal satellite transmission, the audio is transmitted on a subcarrier in the range 5 MHz to 8 MHz. This consumes some of the available power. The EBU system economises by putting the audio in the video waveform. This means that the EBU transmission format is essentially only a video waveform. As a result, the power that would have been used for an audio subcarrier can now be used for the video. This gives a better CNR.

The EBU sound in synch system is essentially a PAL 625 signal with pulse coded modulation, (PCM), data inserted into the horizontal synch section. The PCM data tends to confuse the synch stripping circuitry of some monitors and televisions. This is due to the continually changing nature of the data. The synch detector is expecting a nice clean pulse. Instead it receives a glitchy set of pulses. Some of the televisions and monitors that use edge detection should not have any problems.

Recovering the video on this system merely involves replacing the horizontal synch pulse area in the scrambled signal with a new properly timed horizontal synch pulse. The following is a design idea rather than a complete circuit. The circuit elements have been tested and used in other descramblers.

CIRCUIT IDEA FOR EBU SIS RESYNCHER

PRESET A SETS THE SYNCH TIP REPLACEMENT VOLTAGE.
PRESET B SETS THE THRESHOLD LEVEL FOR THE SYNCH STRIPPER



Circuit Description

A number of circuit elements are required for this operation. The first is a synch stripper. The comparator type given in chapter three is used for this.

The second circuit element is a monostable. This produces the necessary timing pulse to switch out the digital data and reinsert a flat level for the synch tip.

The third section is the video section. This section is somewhat more complex than the previous elements though it has been simplified as much as possible. The input signal to the video section is unclamped video. A video must be clamped for proper processing. The circuit used for this is a typical satellite television receiver circuit. The voltage rating of the Zener is 4V7. The clamped video is then fed to a double pole switch consisting of two 4066 gates.

The function of the electronic switch is to allow the video to be gated through and the digital data to be replaced. The video switch is normally closed except for the period of the digital audio. The digital audio gate is normally open but is closed for the digital audio period. This gate is connected to a preset that sets the synch tip voltage.

The outputs of the two gates are connected to a buffer transistor. The output of the transistor amplifier should be clamped video without the digital audio. It may be necessary to add a field pulse detector and some logic in order to stop the gating triggering on the field pulse section of the signal.

Audio Scrambling Techniques

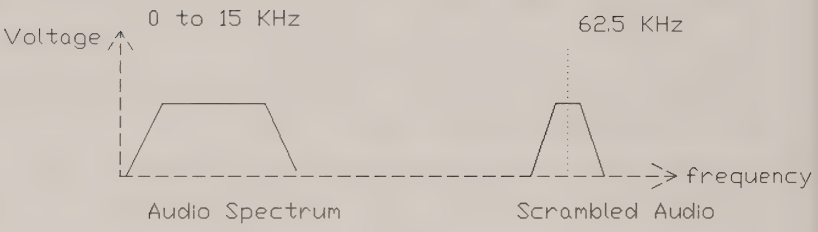
This chapter effectively two sections. The first deals with analogue audio scrambling systems and the second deals with digital audio. At the moment, the only analogue audio scrambling systems in use in Europe are spectrum inversion and spectrum shift. To date the only stand alone digital audio system, other than the MAC systems, has been the FilmNet digital audio system.

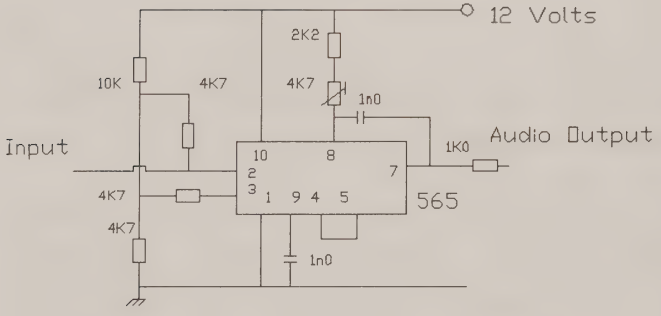
On satellite, the FilmNet digital audio system ceased operation in December 1993. Other digital audio systems are expected in the next few years. At the time of writing there is a report about Sky and News Datacom developing a digital audio dongle that will hang off the back of the decoder or IRD. The options available to Sky are examined later in the chapter.

Scrambling the audio can in itself be an effective measure for low pay services. It tends to destroy the entertainment value of the video unless the video doesn't require any audio track. Another more recent threat to the facility of audio scrambling is multilingual teletext subtitling.

The problem is that audio scrambling on its own is not presently a viable scrambling system and it probably never will be. To date most of the scrambling systems that employ digital audio scrambling tend to economise on the video scrambling. The two more prominent cases of this attitude are VideoCipher II and FilmNet's digital audio. While VideoCipher II had compromised from the outset, FilmNet's situation was forced upon it. The mitigating factor was that the system was supposed to be a stopgap measure until FilmNet went completely D2-MAC EuroCrypt. Unfortunately for FilmNet, their digital audio was hacked and their D2-MAC EuroCrypt system is also hacked.

Digital audio, when examined on its own, is secure. The actual digital audio datastream or signal is secure when being transmitted. This of course is a false security. The point at which a digital audio scrambling system gets hacked is in the authorisation and access control section. A hacker will attack the official decoder and try to make it operate as a pirate decoder. Most of the time, this type of hack will succeed. A classic case of this premise breaking down was the





FM'd Audio Demodulator
62.5 KHz

FilmNet system. In the FilmNet system, a complete reverse-engineering of the hardware and authorisation section was necessary. The final hacker product was better in quality than the official FilmNet decoder.

The VideoCipher II system was hacked because it was possible to hack the authorisation data. The FilmNet digital audio system was hacked because a complete reverse engineering of the decoder was possible.

Any audio system that uses a fixed algorithm and a changable key set is a disaster waiting to happen. This kind of system can no longer be considered secure. It is a frozen architecture therefore it can be reverse engineered. Then it can be duplicated. Then it is up to the scrambling system owner to find the identity of the decoders being used to obtain the keys and turn them off.

Analogue Scrambling Techniques

FM'd Audio

The audio signal is frequency modulated on to a carrier frequency in the range 30 KHz to 100 KHz. The commonest in the US systems are 62.5 KHz, 31.5 KHz, 40 KHz and 63 KHz. While this form of audio scrambling was used in the USA, it has not been used on any satellite systems in Europe.

Descrambling this type of scrambled audio requires a PLL type circuit. There are a number of other types of demodulators but the PLL is the easiest to adapt to this low frequency. The two commonest PLL ICs used for this application are the NE565 and the 4046. The circuit diagram for the NE565 operating at 62.5 KHz is given. The PLL demodulator will need to be preceded by an amplifier as the response of the audio demodulators in most receivers will not be sufficient. Ideally a separate demodulator should be used for the descrambler.

In amny respects this is an antique. It does not offer any decent security. Where it was used, the video was also scrambled, often with a reasonably secure scrambling system.

Spectrum Inversion Circuit
Scrambled Audio In
1496
Vcc
Balanced
Mixer
Carrier Input
Filter
Clean
Audio
Output
See Chapter 3 For Typical Values.

Spectrum Inversion

Spectrum inversion is presently being used by the Discret scrambling system and by the some of the older versions of the SAVE system. The audio on the Nagra Syster is also scrambled using this technique.

This is essentially a single sideband technique applied to audio and was also used for some simple telephone scrambling systems of the late seventies. The descrambling of this system is slightly more complicated than the previous one. The centre frequency, (the frequency around which the spectrum is rotated), has to be recreated.

In the RITC Discret 1 official descrambler, this frequency, (12.8 KHz), is obtained by dividing down the output of an 8.0 MHz crystal oscillator by 625. In the pirate Radio Plans design, the output of a crystal oscillator running at 3.2768 MHz was divided by 512 to produce the carrier. A more elegant method would be phase locking a PLL to the vertical synch. By using a divider of 256 in the VCO - Phase Detector path, the voltage controlled oscillator output would be 12.8 KHz.

The core of the hacker audio descrambler for spectrum inversion is the balanced demodulator. The commonest IC used for this application is the MC1496. The only variations between hacker decoder designs for this type of audio scrambling lies in the carrier generation.

Some designs use the 4060 as the oscillator and divider on a single chip. Others use a separate chip for the oscillator, typically a 4069, and a separate divider. Of the two the 4060 is the more elegant solution.

Spread Spectrum Inversion

This form of audio scrambling is based on the spectrum inversion process. It uses a number of carrier frequencies and as such it can be difficult to hack if all the frequencies are unknown.

Most of the scrambling systems using this type of audio scrambling use one or more crystals to derive the carrier frequency. The descrambler itself derives the video interference carrier from one of the crystal frequencies. The audio inversion frequency is linked to the particular carrier frequency in use at the time. In the SAVE system, the carrier frequency is generally one sixth that of the video interference carrier.

Band Inversion And Rotation

Band spectrum inversion is where the audio spectrum is filtered into different bands and these bands are then inverted or rotated. This is a more secure method than any of the previous ones. It is also more complex and requires a more complex descrambler.

Ideally the audio in each band would be compressed before processing. This system is used in some audio scramblers for use on telephone systems. It is more difficult to hack. The main disadvantage is that the scrambled audio is still discernible in some band rotation combinations.

Spectrum Shift Scrambling

Single Frequency Shift

This is the type of audio scrambling system that was used on the BBC's version of SAVE. It is a more complex system than straight inversion.

To scramble the audio, the complete spectrum is shifted up in frequency by about 1 KHz. To descramble the signal, the scrambled spectrum is shifted back down by 1 KHz. This is generally achieved by Sideband modulation techniques.

The subject is dealt with in detail in the October 1991 issue of Elektor Electronics. A full circuit diagram and PCB layout are given in the article.

Strangely when the article was published, very few people recognised it for what it was. Considering the BBC's legalistic antics when Elektor published the SAVE circuit, this may have been a good thing.

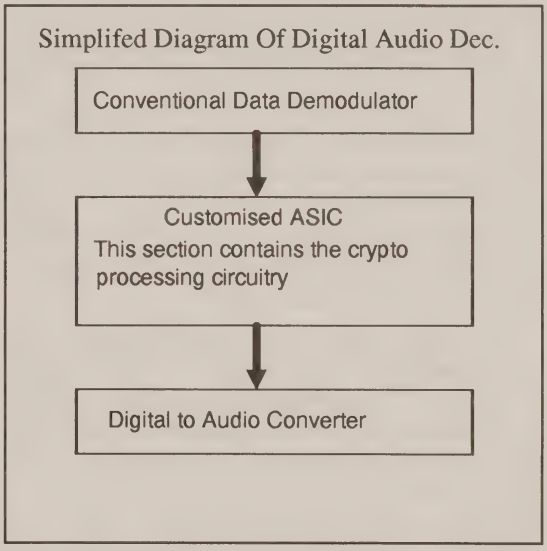
Multiple Frequency Shift

The use of a single shift is not a very secure option. As a result this form of scrambling is more commonly used with a cycling shift. The shift frequency can be derived from a number of crystals or a synthesiser.

Digital Audio

Digitised audio is the hardest type of audio to hack. If the digital audio is encrypted using the Data Encryption Standard, then it will be rather difficult to decrypt.

The architecture of most digital audio systems is simple. The audio signal is digitised and then it is EXORed with the output of a Pseudo Random Binary Sequence Generator. This PRBSG is reseeded every few seconds with a new starting point. In this manner the output of the PRBSG seems to be random. The reseeding data is the key and this is normally the thing that is heavily protected with the cryptographical algorithms.


Simplifed Diagram Of Digital Audio Dec.
Conventional Data Demodulator
Customised ASIC
This section contains the crypto processing circuitry
Digital to Audio Converter

This is of course a very simplifed model but it is also the easiest to implement in terms of hardware. The PRBSG can be constructed as part of an ASIC and the digital audio decoder circuitry can be constructed from off the shelf components.

More commonly, the structure that the FilmNet system used is employed. Conventional circuitry is used to demodulate the data into a serial datastream. This datastream is then fed to a custom ASIC which processes it and then decrypts it. The decrypted data is then fed to a digital to analogue converter.

The use of an ASIC allows the designers more leeway in the choices of crypto systems. While the EXORed PRSG is one of the simplest methods, other more complex algorithms can be incorporated into the design.

Perhaps the more complex solution of using a complete crypto system such as DES to process blocks of digtised audio is not a good one. The decryption process would have to be fast enough not to

affect the synchronisation of the soundtrack and video. Of course it would be possible to adjust the audio so that it is slightly ahead of the video. The inherent delays in encryption and decryption processes would bring the soundtrack and the video back into synch.

There is one system using the DES to encrypt their digitised audio; Videocipher II. This system was hacked due to a flaw in the hardware implementation. The audio crypto system was not hacked. Though it is safe to say that VideoCipher would not have survived in Europe. It is simply too old in terms of technology to be a viable system for the nineties.

Both Orion and Videocipher use pulse coded modulation, (PCM), to digitise their audio. Most of the recent scrambling systems tend to opt for a digital audio. One technique known to be in use is the reverse transmission of digitised blocks of audio information. This type of transmission is secure enough to defeat the casual hacker but will soon fall victim to the dedicated hacker. The key to the descrambling lies in identifying the beginning and end of each block. The digital audio will be encoded according to a recognised data standard. Developing and testing a new data transmission standard for the sake of one scrambling system is rarely economical unless the design team has an extremely large budget.

The commonest combination in digital audio scrambling is a well established data transmission format such as Phase Shift Keying, (PSK), and a customised crypto system. In this respect the first stage of the hack would be the easiest. The encrypted data would have to be extracted from the signal. The second step would be the hacking of the crypto system.

It is common practice to test the digital audio transmission format with clear data. This sometimes causes JAFAs to believe that they have hacked the system while in reality, the system has not been implemented.

There are many types of digital audio format. In this section we shall only deal with two; Adaptive Delta Modulation and NICAM. These systems are currently in use in Europe. Adaptive Delta Modulation is used on the Scientific Atlanta B-MAC system and NICAM is used terrestrially. Though as yet NICAM has not been used as a form of scrambling.

NICAM 728

NICAM stands for Near Instantaneously Companded Audio Multiplex. The analogue audio signal is digitised and is compressed when in digital format. The digital information can then be transmitted in a multiplex format so that mono channels or a stereo channel can be transmitted in the one frame. At the receiving end, the signal is then digitally expanded and converted back to analogue. There are two basic reasons for companding the audio. The first is the reduction of bits required, the second reason is the improved signal to noise ratio in the received audio.

The analogue audio is sampled at a rate of 32 KHz. This is just over twice the maximum audio frequency of 15 KHz. There are 14 bits in the initial audio sample. This 14 bit binary word is digitally compressed to 10 bits.

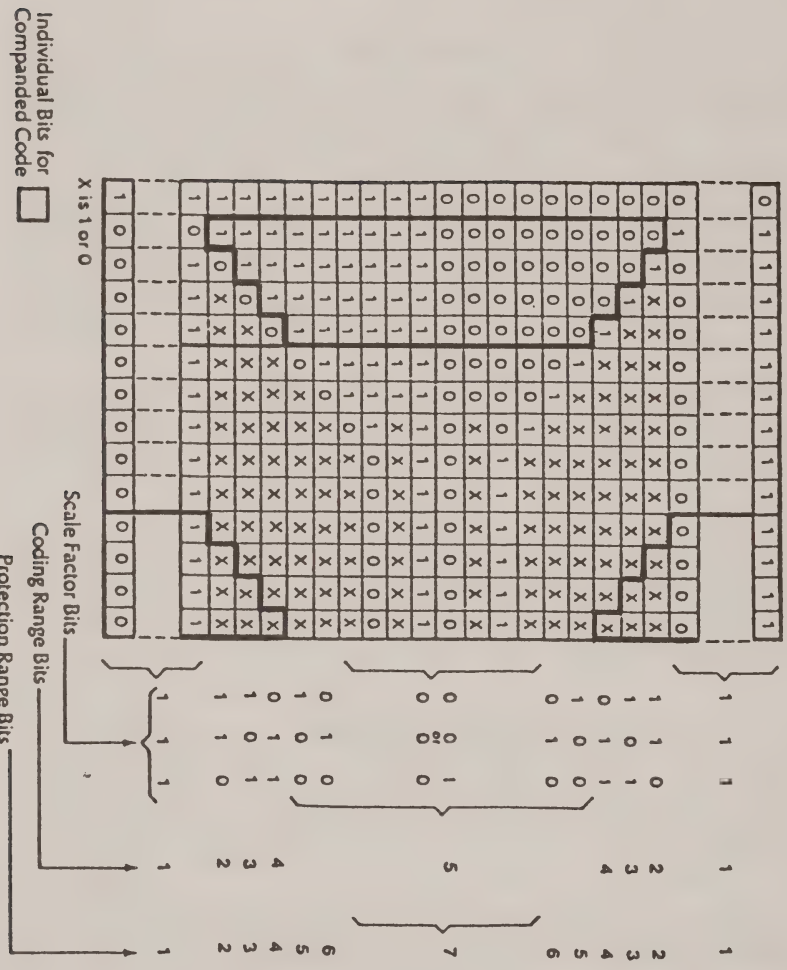
The NICAM system was developed by the BBC in the seventies. The UK version is often referred to as NICAM 728. The number 728 refers to the transmitted bit rate of 728 Kilobits per second. One 728 bit frame is transmitted every millisecond. The breakdown of the bit rate is shown below.

8 bits Frame Alignment Word	8 Kbit/s
5 bits Control Information	5 Kbit/s
11 bits Additional Data	11 Kbit/s
704 bits Sound, Parity or Data	704 Kbit/s
Total:	728 Kbit/s

The first step in the compression procedure is to separate the digital samples into blocks of thirty two samples each.

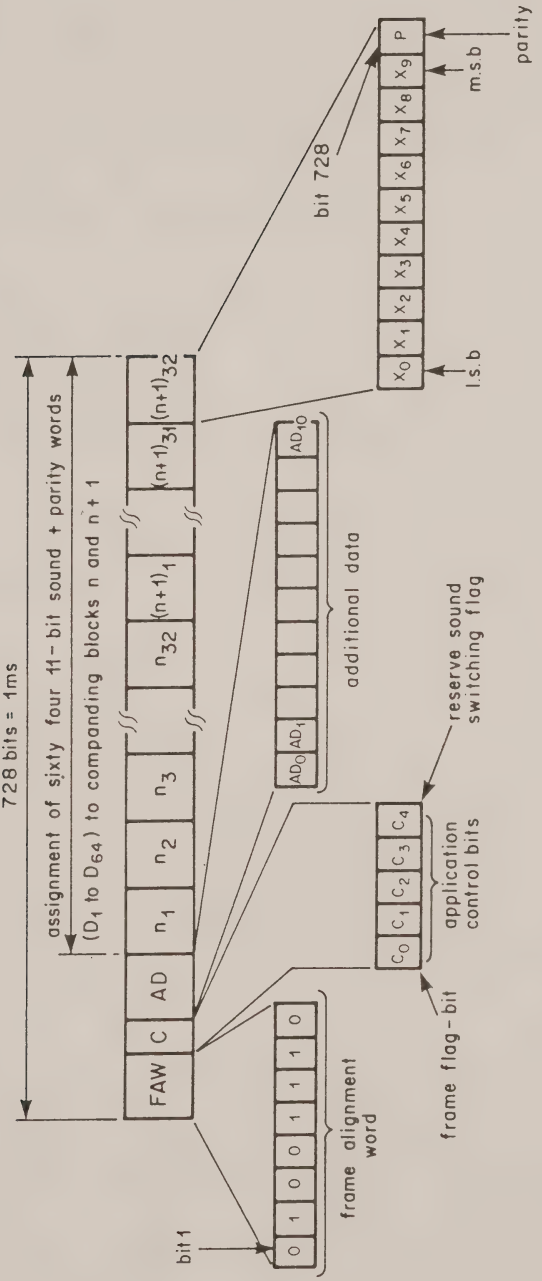
The second step is to code the 14 bit binary samples using a 10 bit 2s Complement code to an accuracy defined by the magnitude of the largest sample word in the block.

The 2s Complement code is an alternative way of representing a number using ones and zeroes. One bit in the number represents the whether the number is positive or negative. This is its sign. The rest of the bits represent the magnitude of the number. This type of representation is called " Signed Number Representation". In this system, positive numbers are represented as simple unsigned binary. There is no change. For a negative number, the situation is different.



The NICAM Compression Chart:

The 14 bit sample is converted to 2s Complement format and then is processed according to the chart shown above. Four bits out of each of the 14 bit wide 2s Complement word are omitted from the final 10 bit word.


728 bits = 1ms
assignment of sixty four 11-bit sound + parity words
(D1 to D64) to companding blocks n and n + 1
FAW
C
AD
n1
n2
n3
n32
(n+1)1
(n+1)31
(n+1)32
bit 1
0 1 0 0 0 1 1 1 0
frame alignment word
C0 C1 C2 C3 C4
application control bits
frame flag-bit
AD0 AD1
AD10
additional data
reserve sound switching flag
bit 728
X0 X1 X2 X3 X4 X5 X6 X7 X8 X9 P
l.s.b
m.s.b
parity

The binary number to be converted is inverted on a bit by bit basis. A 1 will become a 0 and vice versa. Then 1 is added to it. The most significant bit, MSB, of a negative 2s complement number will be 1. The following example will make it clearer.

Example:

To express -7 in 2s Complement, invert 0111,(+7 = 0111). This gives 1000. Add 1, this gives the final value of 1001. Therefore in 2s Complement code -7=1001.

In the third step a Scale Factor is then generated. The Scale Factor tells the receiver which degree of compression is used. The scale factor word is three bits wide.

The Coding Range is defined by the Scale Factor. There are five coding ranges. These are relative to a maximum amplitude of 1.

Range 1:	1 to 0.5
Range 2:	0.5 to 0.25
Range 3:	0.25 to 0.125
Range 4:	0.125 to 0.0625
Range 5:	0.0625 to 0

As can be seen from the diagram, if the block of samples are in coding range 1, the four least significant bits are discarded. For range 2, the three least significant bits are discarded as is the second most significant bit. In each case, the number of bits in the sample is always 10. In this way, the 14 bit samples are first coded into 2s Complement and then into a 10 bit compressed sample.

A further level of information is provided for the receiver by the protection range. This is also related to the Scale Factor. The relationship is shown in the table below.

Coding Ranges	Protection Ranges	Scale Factor r1 r2 r3
1	1	1 1 1
2	2	1 1 0
3	3	1 0 1
4	4	0 1 1
5	5	1 0 0
5	6	0 1 0
5	7	0 0 1
5	7	0 0 0

A parity bit is added to each sample. This is produced by checking the six most significant bits.

The sound and parity bits in the NICAM frame only comprise 704 bits of the 728. The other bits are taken up by the Frame Alignment Word, 8 bits; the Control Information, 5 bits; Additional Data, 11 bits.

The Frame Alignment word is an eight bit word, 01001110, that is transmitted at the start of every frame. Its function is to synchronise the receiver with the datastream.

The control information is transmitted as a five bit block. The first bit, c0 is the frame flag bit. It is high for the first eight frames and low for the next eight. The next three bits, c1, c2, c3 identify the application of the contents of the sound block. The correct term for them is the application control bits. Bit c3 is used to indicate the need for further processing by the receiver. It is this bit that would be used to switch in the decryption circuitry in the receiver. If the bit is high and the receiver does not have the necessary decryption circuitry, then the audio output will be switched off. The fifth bit c4 is the reserve audio switching flag. This bit is high when the FM subcarrier is carrying the same channel as the NICAM.

Application Control Bits Table

Data Contents Of Sound Blocks	
c1 c2 c3	
0 0 0	Stereo signal. Alternate samples.
0 1 0	Two Mono channels, M1 and M2, alternate frames
1 0 0	One Mono audio and one data channel, alternate frames.
1 1 0	One 704 bit data channel

There are eleven additional data bits. The function of these bits has not been defined. It would be easy to use them as a service identifier or for transmitting other data.

The modulation format used to transmit NICAM, terrestrially, is Differentially Encoded Quadrature Phase Shift Keying or DQPSK for short. This is a rather elegant modulation system in that it reduces the bandwidth required to transmit the data. Each phase change represents a bit pair or two bits of data. The following diagram shows the rest state of the carrier phase. The rest states are ninety degrees

apart. The carrier phase remains in one of the rest states until a bit pair causes it to change phase by the predetermined amount. The phase change caused by each bit pair is shown in the table.

Carrier Rest States Bit Pair - Phase Change Table

1 Bit Pair Phase Change

A	B	Phase Change In Degrees
0	0	0
0	1	-90
1	0	-270
1	1	-180

With the carrier in rest state 1, a bit pair of 10 will cause a phase change of -270 Degrees. This would put the carrier phase in rest state 4. Applying a further bit pair of 11, would cause a phase shift by -180 Degrees to rest state 2. Applying a further bit pair of 01 would cause a phase shift of -90 Degrees to rest state 3. Strangely, the negative shift is clockwise.

The modulation format is clear and unambiguous. A bit pair can always be recovered by comparing the present phase of the carrier with the immediately previous phase.

Before the 728 bit frame is converted to bit pairs, the datastream is scrambled for spectrum shaping purposes. This is carried out to ensure that the data looks like noise and so causes minimum interference to the video or other audio carriers. A pseudo random sequence generator is EXORed with the data stream. The PRSG is a nine stage type. The initialisation word is 111111111. The Frame Alignment Word is not scrambled. The first bit that is scrambled is the bit immediately after the Frame Alignment Word and the last bit that is scrambled is the bit immediately before the FAW. The descrambling of the frame must be carried out at the receiver before the multiplex is split up.

Since the information is in digital format, it is easy to encrypt. The simplest method is to encrypt the Frame Alignment Word, FAW. This would ensure that a NICAM descrambler that didn't have a valid FAW couldn't lock up the frame. The NICAM digital signal is EXORed with a PRSG bitstream for noise reduction purposes. This PRSG has a fixed seed. If a variable seed is used, a simple though efficient encryption

system could be effected. The keys for the encryption system could be held in the descramblers or transmitted in the unassigned bits in the NICAM signal.

The NICAM format could easily be adapted to a satellite television application. The first and most obvious modification to the standard is the carrier frequency. The carrier frequency for NICAM 728 as used in the UK is 6.552 MHz. This frequency is obtained by multiplying the transmitted bit rate of 728 Kilobits per second by 9. By multiplying the bit rate by 10, a carrier frequency of 7.28 MHz would be obtained. The bandwidth of the NICAM carrier on the UK terrestrial system is 700 KHz. The beauty of this modification is that only necessary modifications to a normal NICAM demodulator are the carrier crystal frequency and the input bandpass filter.

Adaptive Delta Modulation:

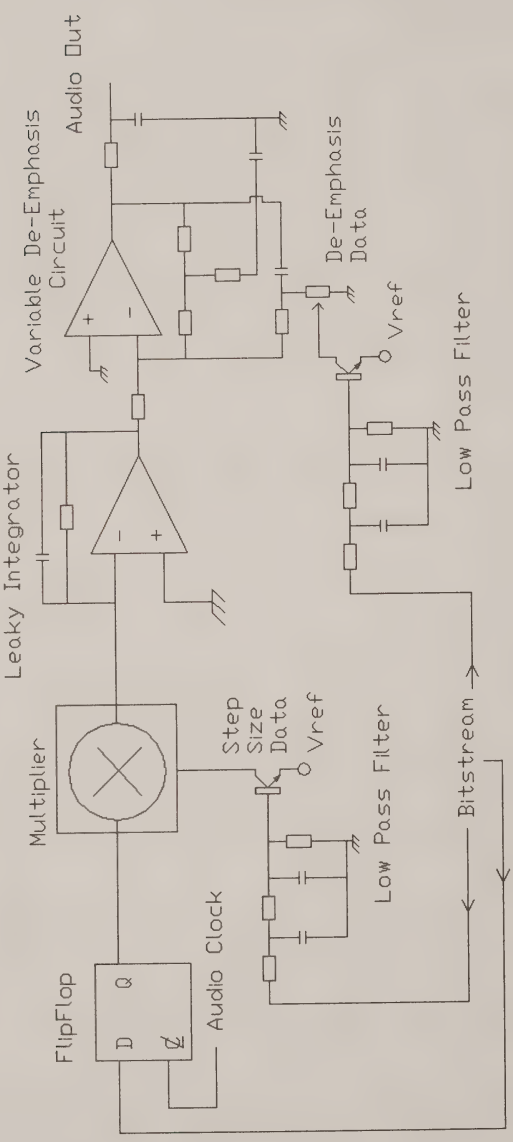
The Adaptive Delta Modulation format was developed by the Dolby Laboratories. It is used on the Scientific Atlantic B-MAC system. This system is currently employed on the AFRTS and the SIS Racing channel.

Delta is used in mathematics to indicate change. In a delta modulation system, the delta refers to the direction of the change. The delta would be positive or negative. There is a disadvantage associated with ordinary delta modulation systems. When the amplitude of the audio signal changes by an amount greater than the quantizing step size, (the minimum voltage change required to effect a one bit change in the digital output of the analogue to digital converter), an overload occurs. Adaptive delta modulation overcomes this problem by using a variable step size and a variable pre-emphasis.

At the encoder, the audio input is continually monitored so that the best step size and pre-emphasis can be selected. The adaptive delta modulation produces a bitstream of between 200 and 300 Kbit/s. The step size and pre-emphasis data are transmitted at a lower bit rate. This makes the design of a decoder simpler.

The slower bit rates of the step size and pre-emphasis data allows them to be filtered out with simple low pass filters. As can be seen in the simplified adaptive delta modulation decoder, the decoding process is straightforward. The digital audio data is fed into a flip flop. This flip flop is clocked by the audio clock. The output of the flip flop is

Simplified Adaptive Delta Demodulator



either 1 or 0. The output is fed to a multiplier. The multiplier is an analogue circuit that is used to form the product of two voltages. The multiplication factor is set by the step size data. The output of the multiplier is fed to a leaky integrator. The output of the multiplier is essentially a set of discrete voltage points. The leaky integrator joins these points to give a smoother signal. The output of the leaky integrator is then fed to the variable de-emphasis circuit. The resultant audio is then amplified and fed to the modulator or audio output.

An adaptive delta modulation decoder is available in chip format as the NE5240. This is a stereo decoder and is used in the B-MAC descramblers manufactured by Scientific Atlanta. In these descramblers the digital audio must first be decrypted before being converted form adaptive delta modulation format. The encryption system used in the B-MAC system is a variant of the Data Encryption Standard. It is also more secure than the DES. Nobody has commercially hacked the audio on this system.

Duobinary Encoding:

The Duobinary encoding system is a relatively simple method of encoding data. It allows for the even simpler design of the decoder. It is used in the D-MAC and D2-MAC systems. It is a baseband system that conveys data by the level of a three level waveform. This analogue-like appearance means that it can be frequency modulated for satellite television transmission along with the reset of the MAC signal. The disadvantage of the C-MAC system was that it required the video section of the line to be frequency modulated and the data section to be 2-4 PSK modulated. This meant that two demodulators were required and the encoding circuitry was over-complicated.

In this section we are concerned with digital audio. D-MAC and D2-MAC are covered in detail in Chapter 7. In D-MAC there are 209 data bits in each line's sound and data packet. In D2-MAC there are 105 bits in each line's packet.

A duobinary encoder can best be considered in three stages. The overall process is a combination of digital and audio techniques.

The first step is to pre-code the bitstream. The bitstream is inverted. Each bit in the bitstream is then EXORed with the bit immediately previous. The new bitstream is then fed to a level shifter. This produces a +1 and -1 bitstream.

The second stage is part of the encoder is the encoding section. The pre-coded bitstream is subjected to a one bit delay and added to itself linearly. The resultant signal is amplitude limited so that it cannot exceed the maximum video level.

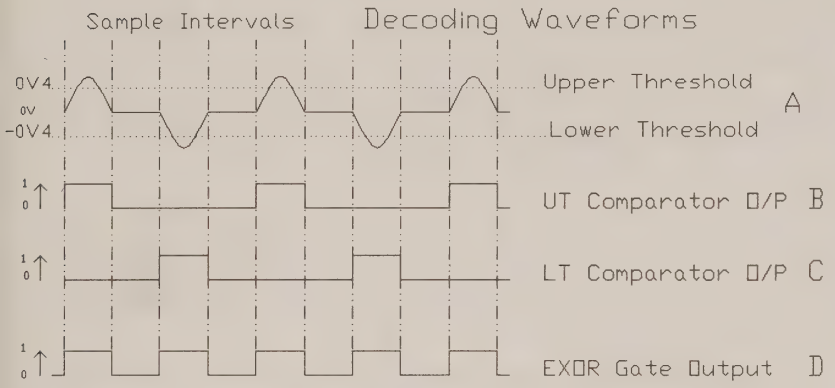
The third stage is the low pass filtering. This is essential if the bitstream is not to produce harmonics. The other reason for the low pass filtering is to reduce the bandwidth required for the D2-MAC sound and data packet to approximately 5.026 MHz. In the D-MAC system, the filter limits the D-MAC sound and data packet's bandwidth to approximately 10.5 MHz.

The levels of the duobinary encoded signal are +0V4, 0V and -0V4. Logic 1 is represented by 0V4 and -0V4. Logic 0 is represented by 0V.

The operation of the duobinary decoder is extremely simple. In theory, it consists of two comparators, an EXOR gate and an inverter gate. The duobinary signal is fed to the two comparators. One comparator slices the signal at the upper level. The second comparator slices the signal at the lower slicing level. The outputs of the comparators are fed to the EXOR gate. The output of the EXOR gate is inverted by the inverter gate and the original bitstream is restored.

The data slicer is generally on the integrated circuit rather than being discrete circuitry.

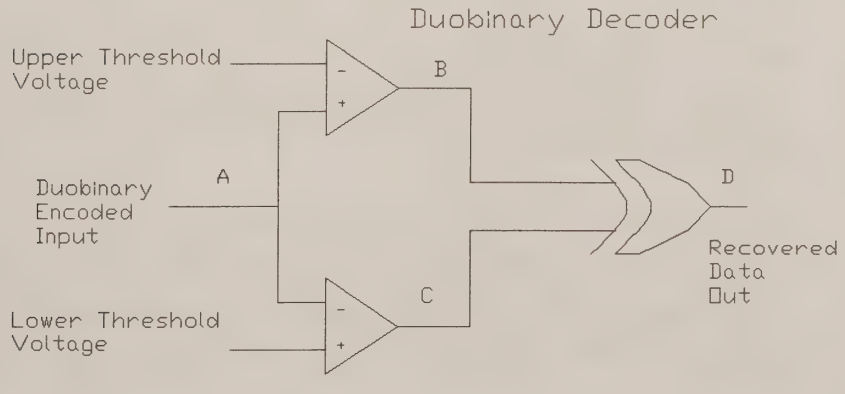
Duobinary Decoding (D-MAC / D2-MAC)



The top waveform, A, is the actual duobinary encoded signal. It is a tristate signal. The levels used are 0 Volts, +0V4 and -0V4.

The comparators in the diagram below slice the duobinary signal at the upper and lower thresholds. The outputs of the comparators are waveforms B and C. These waveforms are EXORed using the EXOR gate. The output of the EXOR gate is the recovered data.

The process of decoding a duobinary signal is simple when compared to the modulation system used in B-MAC or C-MAC.



VideoCrypt Digital Audio?

According to some reports, Sky intend to launch an add on to their system in the event of a hack on the 09 card. This add-on will apparently be a digital audio dongle that connects to the SCART socket on the back of the decoder or IRD.

The report went on to say that this device will be manufactured in the UK by GEC. In early June it was at prototype stage though a production type would be available by September.

The problem with this report, even if it is true, is that it looks like a very strange move. The VideoCrypt system was initially specified with a very low grade analogue audio scrambling. The introduction of digital audio at this late stage in the proceedings would be rather stupid and that is a worryingly convincing aspect of all this.

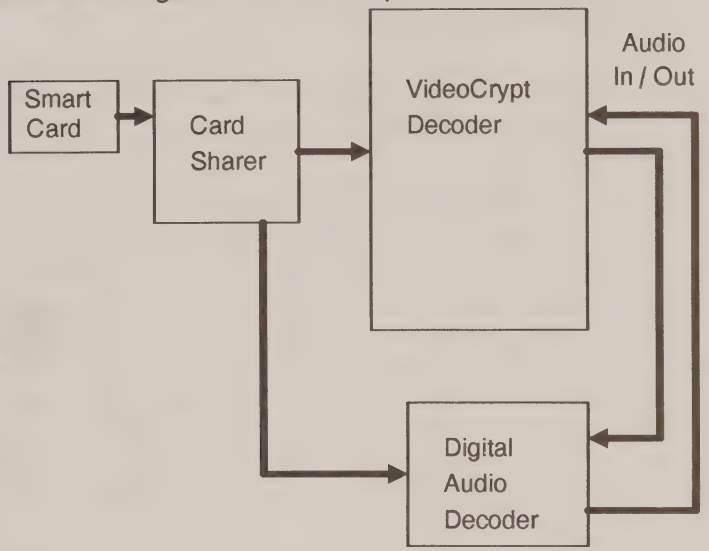
Let's play along with the report for a while. The Sky channels would have at best three audio channels to encrypt: the mono audio channel and the two stereo channel. If they could sort out some form of control channel, then the other remaining channels could be used to handle the digitised audio. This would be marginally possible though a dumb version would be more likely as it would remove the need for the extra overhead of control data.

Naturally their design would be as customised as possible with the use of ASICs. FilmNet had a similar idea. Their digital audio system was utterly smashed and the ASIC was reverse engineered. If indeed Sky and News Datacom do manage to bring in digital audio, it will have a very limited lifespan.

The product under development may well be a digital radio system with smart card control rather than a completely new digital audio system for the VideoCrypt scrambling system. This could be pressed into service as an audio scrambling system for VideoCrypt but it would be a waste of resources.

If it was smart card controlled then the customer would need a second smart card or some kind of card sharing technology would have to be used. The card would plug into a card sharer interface and the datastream would be split between the decoder and the digital audio decoder. There are some commands to and from the smart card that are presently unused which would possibly be used in this approach.

A Possible Digital Audio Set-Up



The problem with this model is that the card datastream has to be shared between the VideoCrypt decoder and the digital audio decoder. There are a few commands that have not been used in the VideoCrypt system that could be used in this application.

The main task would be to make the card sharer aware of the command directions so that it could decide if the card instruction was intended for the video decoder or the audio decoder.

This type of technology is possible to implement though it remains to be seen what commands will be used to control the digital audio section. The unlisted card commands in the new 09 card might have something to do with the card personalisation process than a digital audio system.

In the FilmNet system, the control channel was separate from the digital audio channel. The smart card would allow a similar architecture for this VideoCrypt digital audio system Instead of having to rely on a subcarrier, the control channel would be transmitted in the video sigal as part of the main access control channel. There are more possibilities with this digital audio system in terms of crypto.

At the moment, all of this is only speculation. There is no reliable confirmation on the use of digital audio by Sky. As a result this model is only a hypothetical one.

The most common form of digital audio encryption is a digital audio datastream EXORed Pseudo Random Number Generator. This is the kind of system used in D2-MAC. It is also one of the easier types of system to implement.

The crypto architecture may also follow a more conventional structure. If the digital audio system is only in prototype, there is not really enough time to have developed a truly awesome system.

In order for the security of the system to be of a reasonable level then the key system must be continually changing. This idea can be seen in the way the decrypt key for the video descrambling is generated every 2.5 seconds. In the audio system, this frequency of key generation would not be a good thing as it is really too fast to allow the use of a hard encryption algorithm such as RSA or perhaps a verification algorithm like the Fiat Shamir Zero Knowledge Test. (See chapter 6 for details).

The main problem with RSA is that it is processor intensive. The multiplication and exponentiation takes a lot of time in terms of a microcontroller or processor. The Fiat Shamir ZKT also suffers from similar problems.

Using the RSA would mean some form of distributed processing had to be used in the digital audio decoder. On processor would control the crypto information and generate a new key every fifteen minutes or so. The other processor would handle the housekeeping. After the crypto processor has generated the key, it would be written to RAM in housekeeping processor or indeed in the crypto ASIC.

It would be logical to hide all of the main processing functions in the ASIC rather than in easily popped chips. The Fiat Shamir ZKT or some other authentication routine would have to be incorporated in order to personalise each digital audio decoder.

Again at this stage it is too early to tell if the reports are correct. But given that the European Blackbox Industry is more powerful in terms of people and processing than News Datacom, a digital audio system would be a relative dead end.

Information Acquisition

To the uninitiated, hackers seem to able to lift information about systems by magic. Marketing executives are particularly prone to this sort of paranoia, especially when they begin to believe their own advertising copy. About ninety eight per cent of the information required to hack a system is freely available. It is simply a question of knowing what to look for.

The best place to hide something is in plain sight. This is a good example of lateral thinking. The searcher will be looking for something that is hidden and since the thing is not hidden he will not find it. Most of the time this line of thought appears to work.

It has been said that electronics is merely a set of modules. Electronic engineering is knowing how to interface these modules. Hacking involves being able to take the modules apart and then put them back together.

Continuing this line of thought, a scrambling system is an arrangement of modules that produces a specified output from a known input. Most systems designers will use a tried and tested module rather than developing a new one. With totally new circuitry the business people in the company will try to have the design patented. In doing so they provide the hacker with an easily accessible source of information. The companies often try to protect themselves by reducing the circuit to IC level. The hacker has the advantage of knowing that the development work was carried out using discrete circuitry.

This is the information acquisition section of the chapter. In hacking, information is the most valuable commodity. Strangely for such a valuable commodity it is often badly protected. The actual term "Information Acquisition" is a catch all phrase. It basically covers information gathering, analysis, and no small bit of wizardry

In order to acquire information, it is best to know where it lies. There are basically three types of information: published, electronic and and holistic. Ideally every piece of obtainable information on a system should be considered when assessing the security of that system.

Published Information Sources:

Published information is that derived from the technical and non-technical media. The brochures from the system manufacturers are also in this category. While the information in the technical and trade magazines is generally accurate there are a few journalists who are more a liability than asset as an information source. These journalists tend to work for the advertorial and social studies magazines.

In satellite television and scrambling in Europe, there are basically a few magazines and newsletters that are essential. The first newsletter is obviously Hack Watch News. This is the only newsletter on signal security in Europe. It is to paraphrase the MAD motto "First in a field of one."

The best newsletter for market intelligence is "Interspace". This newsletter is the oldest newsletter on cable and satellite television in Europe and has the highest quality information on the satellite television market. It is a weekly periodical so the information is still relevant when you get the newsletter.

The best newsletter on satellite activities in Europe is, without doubt, "Transponder". The newsletter is published twice monthly and contains the most accurate accounts of television and radio traffic on satellite in Europe.

The 21st Century Publishing title, "Satellite Trader", carries the Syndicated Hack Watch each month. This is my syndicated column and Satellite Trader is the UK paper publisher for it. The equipment reviews in this magazine are generally non-technical and written by JAFAs. The news content has improved over the last few years.

"What Satellite" is perhaps one of the best gauges of the public perception of satellite television. It is a glossy magazine aimed at a general readership. The equipment reviews are good though have minimal technical content. The news is generally culled from other sources but the strong point of the magazine is that it frequently carries excellent articles on programming.

There are of course other magazines covering the business side of satellite and cable television. Among these are the titles Cable and Satellite Europe and Satellite and Cable Communications International.

Cable And Satellite was at one time the best satellite and cable magazine in the market. There was a balance between technology and business. Unfortunately this has changed for the worse over the last few years. It is now considered to be mainly an airhead magazine for the bizoids. Some hackers have even gone as far as to label it a room temperature IQ magazine. This is of course overkill. The magazine frequently carries excellent articles on cable television and legislation.

Most companies in electronics crave publicity for their products and so will seize every opportunity for a bit of free advertising. Professional journals, that is those aimed specifically at engineers, designers and buyers, are the most reliable sources.

Some of the magazines intended for hobbyist can contain some useful information but should be considered with caution as the data has been simplified possibly by someone has very little knowledge of scrambling systems. Newspapers can provide the names of the scrambling systems used by various cablenets. Generally it is the provincial papers that would carry this type of information though the national papers can sometimes pick it up. The person who gives this data to the journalist is almost invariably the system manager and non-technical. They love to boast about their brand new high security scrambling systems that will prevent the pirates from tapping their system.

The non-technical person can be one of the most helpful sources of information for the hacker. In system manufacturing companies, they generally offer to send you the full technical data and or brochures. With some it is better to be a student doing a project on scrambling systems as people generally like helping others. As detailed in chapter one, the non-technical person can give away the the full data and strengths of their scrambling systems without even knowing it. This kind of information acquisition has more to do with social engineering than published information.

Electronic Information

The electronic information sources are the more valuable. They are more immediate as the printed and video media is often between one week and three months out of date. The electronic information sources include bulletin boards and on-line information sources.

The world of electronic information has been referred to in the Cyberpunk novels as "The Matrix". This is a fairly accurate if somewhat poetic description. Most of the sources of electronic information are linked in some way. The commonest method of accessing the sources is via dial-up modem.

There are basically two forms of electronic information sources; bulletin boards and on-line data exchanges. Naturally the bulletin board or BBS is the most common.

At its minimum, a BBS is a computer, a hard disc and a modem. It is possible to dial in, leave messages and upload and download files. the files can be anything from porn to games programs. Most of the good generalised boards tend to have a wide mixture.

Special Projects BBS (+353-51-50143) is a BBS that specialises in satellite and cable television and scrambling. Most of the information and files on this BBS are free. Some are only available to subscribers. The following pages contain a list of the "interesting" files available.

Hack Watch News - Technical Files Section

SM_DIAGS.ZIP

Circuit diagrams of the D2-MAC smart card test rig. These files are in GIF and PCX format.

SMART-01.ARJ

Smart card test rig for D2-MAC smart cards. Contains details of card information and runtime version of interface program. The text is in Swedish.

SMART02.ARJ

Print files for D2-MAC smart card test rig in epson and postscript format. The postcript format file will print out but the epson does not.

SMART-03.ARJ

Smart card test rig for D2-MAC smart cards with PASCAL source files.

OMIGODSC.ZIP

Source Code in C and ASM For Version 1.2 OMIGOD. This hack is also known as SEASON7.

DDT_SC.ZIP

Source Code in C for the DDT Hack. This hack is also known as SEASON13.

16C84ASM.EXE

Full listing of a PIC16C84 program for decoding the Sky channels (07 Smart card issue - does not work with 09). A very good example of how the hack works.

PHREAK.ZIP

A history of Phreaking This is the Official Phreaker's Manual from 1987. It is interesting from a technical point of view in that it gives some very good descriptions of the technology. It also includes some articles on phreakers.

9346PGMR.EXE

9306 & 9346 EEPROM Programmer and cct

SKY.ARJ

The Morley Research Hack as featured in Black Book 3and 4.

DIS6805.ZIP

6805 Dissembler Program

PIC Microcontroller Files

PICPROG.ZIP

Serial PIC Programmer (Printer Port) This program allows the construction of a very simple interface to program the PIC16c84 chips serially. The printer port, LPT1, is used in a serial manner. The interface is based on a single 74LS07 hex buffer.

I2C.SRC

Source listing for i2c implementation in PIC

XMIT232.SRC

Source listing for implementing RS232 transmit in PIC

RCV232.SRC

Source listing for RS232 receive routine in PIC

EEPROM.SRC

DIGSCOPE.SRC

ASPIC.TXT

Text file on the PIC Assembler Program

ASPIC.ZIP

Shareware PIC Assembler Program that also covers some other microcontrollers. This is an excellent program and well worth the registration fee.

PMA.ZIP

PIC Macro Assembler

PSIM_5X.ZIP

PIC 16c5X Simulator Program

PSYM.ZIP

PIC Simulator

PIC16C5X.ZIP

PIC_C.ZIP

C to PIC Assembler

TALK.ZIP

PIC To PC Communications Program

ALL_APPS.ZIP

Applications notes on PICs from Parallax BBS.

TABLE.SRC

Example of Look-Up table implemented in PIC assembly language.

DISASM.ZIP

Disassembler for PIC 16Cxx and 17Cxx microcontrollers

VideoCipher II And Other US Systems

ENDECODE.ZIP

Program used to decrypt and encrypt seed information.

RS232.ZIP

Interesting file on how to hook up a VideoCipher II decoder to a computer via an RS232 interface. Would make interesting reading for anyone interested in using a PC to snatch data from any decoder. The graphics are in ASCII with full text

VC2PC.ZIP

File on connecting the VideoCipher II decoder to a PC serial port.

EASYVC1.ZIP

Video Only Descrambler design for VideoCipher II.

CABLEFIX.ZIP .

Cable Hacks On US Jerrold Systems.

CT_CPIR1.ZIP

How The Salora Cable Decoder Was Hacked.

There are electronic mail networks that allow messages to be entered on one BBS in, for example Ireland, which will reach someone on another BBS in the USA. Most of these mail networks are free. The commonest one is FidoNet. This is a network that spans the planet.

The BBS scene is small compared to the Internet. There are many good books available about the internet among them Ed Krohl's "The Whole Internet User's Guide & Catalog". There are a number of relevant newsgroups which cover satellite television. The best way to consider these is as discussion groups. In some respects they are electronic mail networks.

The most important newsgroups regarding satellite are:

alt.satellite.tv.europe (European satellite television)

rec.video.satellite (US satellite television)

Other newsgroups of interest would be:

sci.crypt (Cryptology)

sci.electronics (General electronics discussions)

Holistic Information

Holistic information is essentially taking the whole view of available information sources. Perhaps the best way to define it would be as the connections between the information. Of course to those not in on the secret it is wizardry.

The secret is to watch, read and analyse everything that you can get your hands on. After a while, patterns begin to emerge. The following paragraphs on the issue of the 07 Sky smart card best illustrate the concept of Holistic Information.

Figuring out what a channel is up to can be akin to crystal ball gazing. The analogy is not totally inaccurate. It is in a sense fortune telling but these days it often known as futures analysis and the crystal ball has been replaced by a computer screen.

Sky's issue 07 card was supposed to be top secret. It was perhaps the worst kept secret. For a start, the news was inadvertently leaked. At this stage the story was as solid as interstellar space.

Sky's change of smart card came as no surprise to hackers. It had been announced in a manner similar to the FilmNet gaffe. Perhaps extracted would have been a better description.

5: Dirty Tricks

At the Subscription Television Conference in June 1992, I stated in a paper on hacking and piracy that VideoCrypt had been hacked by limiting the EPROM write voltage. Up to that date News Datacom had totally denied the hack.

In the questions and answer session that followed the presentation, the head of France Telecom's Visiopasse program, Jean Pierre Coustel asked if anyone could corroborate what I had just said. A News Datacom delegate rose to the bait.

For the first time someone from News Datacom had admitted, on the record, that the VideoCrypt system had been hacked. After a few seconds of cross examination, the delegate said that it was not the fault of News Datacom but rather the chip manufacturers. He also said that the 06 issue of cards had countered that hack. Then came the mistake. He said that all this did not matter as they were going to change manufacturers. The first piece of the puzzle was in place.

By August, the card programming factory was being refitted with new card programming and testing equipment. The trucks were moving in the gear in a style of a particularly bad World War Two movie. The people going in and out of the buildings were searched. Journalists were specifically excluded from the area.

Sky had got it wrong. The threat to their security did not come from the journalists, it came from the hackers. They assumed that they were dealing with an ordinary average foe. Hackers are far from average.

By analysing what was happening with the way journalists were being handled by Sky, interesting patterns started to emerge. People in Sky were becoming less and less talkative. The lack of candour was partially attributed to the fact that a journalist on a staid journal quoted a source in Sky by name. The source apparently was speaking off the record at the time. As with everything else in signal security there was an undercurrent of intrigue.

When a usually talkative company gets corporate laryngitis, something is going on. The fact that journalists were being excluded from various areas confirmed this. The second piece of the puzzle was in place.

At this point some of the best hackers in Europe made a break though. The KENtucky Fried Chip appeared on the scene. The smart card interface in the VideoCrypt decoder is controlled by the 8052

microcontroller. This IC has 8K of program memory. The version used in the decoder was a ROM type but in a stupid oversight, News Datacom had neglected to protect the program. Anyone could dump out the program. The KENtucky Fried Chip was a rewritten 8052. The routines to switch off the card had been modified. Sky had lost control over their access control system.

Sky were obviously disturbed at this development but it was not pursued as vigourously as it should have been. It seemed that Sky had something up their sleeves. They did manage to nuke version 1.0 of the KFC but this was to be expected. In fact it was intended.

They did not nuke version 1.1. This was the version that would be released to the general public. For a company facing a hack of VideoCipher proportions, Sky were awfully smug. This smugness was the third piece in the puzzle.

European Grey Market operators began to notice that it was more difficult to get the Quick Start cards. Even the ordinary smart cards were getting more difficult to acquire. Some commented that this type of thing usually heralded the issue of a new card. This was the final piece of the jigsaw.

It can be seen from this that figuring out what a channel is up to is not difficult. It does require information from a wide and varied set of sources. The trick is learning to collate and assess the underlying motives and reasoning inherent in the information.

This ability is natural in most parts of Ireland. In Ireland it is what is not said in a conversation that is the most important. What most people seem to forget is that English is a relatively crude language that has only truly been in existence as a stand alone language for about six hundred years or so.

The Irish language and mindset has had the advantage of thousands of years of history and evolution. Incidentally Irish is actually the third oldest written European language. It was developed for the expression of abstract concepts and ideas. English is a more utilitarian language as its basic threads are French, Latin, German and Irish. As a result attempts at obscuration in English can be woefully transparent when examined with an Irish mindset.

If you want an example of the mindset, take the Blarney Stone. Its quite an achievement to have people kiss an antique latrine for that is actually what the Blarney Stone was.

Social Engineering - The Human Factor

In hacking, a Social Science number is a large number devoid of meaning. They look good on a report and the bizoids just love them. Social science has a particularly low respect among hackers and the term "Social Engineering" reflects this. It is a euphemism for making a person do what you want them to do without them knowing why they are doing it.

In this respect there is common ground between hacker, journalists and spies. A hacker has to extract critical information about a system, so a good place to start is the manufacturing company.

Telephone calls generally produce the best results as letters are generally filed and followed up for possible sales. Another possibility is to be a free-lance journalist working on a scrambling systems article. Most electronics magazines depend on freelancers for their articles and so the company may be prepared to help.

With some professional hackers, a common phone tactic is to use a male enquirer if the company contact is female and vice versa. A good accent and phone voice can be essential for this kind of information acquisition. The best kind of accent is one that can readily be understood in all areas of a country but cannot be identified specifically with any particular area. An assumed accent can be deadly. Most people can tell a fake accent. If a contact cops on to the fake accent the conversation will quickly be terminated. The majority of the selected contacts are what the English would call middle class. Many people tend feel more comfortable with a person whose accent is similar to their own. A common tactic here is to absorb some of the terms or colloquialisms used by the contact and reuse them in the conversation. In a large cable network for instance, the local technical manager is unlikely to be what the English would call middle class. He is not likely to have a University or RTC education. Using a middle class accent to gain information from such a person can be counterproductive.

Trade shows are also useful for obtaining information. These are mainly for bona fide business representatives and at some, free-lance journalists are not welcome. These require the hacker to be a legitimate business person. In some cases, this may be possible. All professional hackers are legitimate business people.

Most of the top professional hackers are consultants and so get maximum co-operation from the representatives of the system manufacturers hoping for a good recommendation and a commission. Most of the real information is let slip in the bar after the show is over for the day. Alcohol tends to soften the brain and loosen the tongue. Always drink a non-alcoholic drink at one of these occasions and watch out for the smart sales-rep who tries to force you to have "something stronger". If it is not possible to stay around for the after show drinking, then it is best to arrive late in the afternoon as the sales-rep will be tired and more likely to make a slip. Some shows allow the visitors to pay at the door but they do require some business identification.

At most trade shows, there are after show receptions. Generally, these are cheese and wine affairs and the trade show representatives will mingle. Of course at this stage they are extremely tired.

A standard procedure is to target a specific representative. This is where things get cold and cynical. The alcohol in white wine and champagne is in a freer form. It is more rapidly absorbed into the bloodstream. By offering to get the drinks, there is a chance to get the representative to drink white wine. Information extraction is faster as the combination of alcohol and fatigue quickly reduce a persons resistance.

One of the most helpful sections of a scrambled channel is the publicity department. These people are there to help and some of them are wonderfully naive - something that hackers tend to take advantage of. Over the last few years, there has been an increase in the security of some channels. They actively engage in disinformation. The public relations department usually handle this information though they are commonly unaware of the content or relevance of the data.

It appears that a prerequisite for employment in a public relations department is that the person must be pleasing to the eye. This has saved more than one channel during a few INFOACQ operations. One hacker, intent on extracting the maximum amount of information from a contact in a public relations department completely forgot about the operation when he met her at a trade show. Luckily he did not blow the operation.

In social engineering there are essentially two rules; everybody wants to be noticed and people like to talk about themselves.

Above all everybody, from secretary to boss, wants to be seen as someone who matters, someone who has power. Its a basic human need. They want to use that power. If you give them the opportunity the chances are they will use it to your benefit.

Most of the biggest successes in information acquisition came about not by pouring through mounds of paper but by listening to what people say.

Counter Piracy

In any hack there are two sides; the hackers and the counter pirates. I use the term counter pirate rather than counter hacker because the counter hacker is the actual system designer. Counter piracy is necessary when the hacker succeeds.

The first stage in the counter piracy procedure is to examine the problem. This generally comes under the heading of threat analysis. Threat analysis deals with identifying the threats that a scrambling system will face and the most effective methods of neutralising these threats. Some of the threats and solutions will be of an extra-legal nature.

This kind of work cannot generally be undertaken by anyone who is not or has not been a hacker. It requires the ability to think like a hacker.

The decision to cope with piracy is one that when taken cannot be revoked. It requires the company to pursue the fight until the bitter end. Once the program is initiated it must run to its logical conclusion, the elimination of all piracy threats.

Melodramatic stuff indeed! Despite its melodrama it is true. When a channel scrambles, the threat of piracy is always present. The company must decide whether it actively wishes to stop the piracy of its signal or to sit back and hope that the threat of random changes to the scrambling system is enough to deter the commercial pirates. The histories of scrambling systems have shown us that commercial pirates will not be deterred by the random upgrade threat. The upgrade generally has an active lifetime of two to six months. After that time, the situation will be similar to the one that existed prior to the upgrade.

A counter-piracy operation is not a cheap operation. Any non-tech consultant who claims otherwise is an idiot. There will of course be cries from the non-tech "experts" such as those in advertising and marketing claiming that piracy can be stopped by legitimate means such as injunctions. These people are not living in real time.

A counter-piracy operation does not limit itself to legal action against the pirates, it sets out to destroy the pirate's operation by whatever means that are available. It is in effect a war and in a war you cannot partially kill your enemy.

The selection of the correct people is the cornerstone of the counter piracy operation. Unless the company is extremely lucky, these people will not be found among the employees of the company. Even if people with suitable talents exist inside the company they should not be used. They can actually be linked to the company. The pirates would have no qualms what so ever about destroying the channels name in the press. Since the counter piracy operation may be using extra-legal techniques, the consequences of implication for the channel could prove fatal.

The rest of this section will begin to read like a chapter out of a spy novel. The techniques are similar as they have already been tried and tested in such real life scenarios upon which spy novels are based.

The number involved in the planning of such an operation must be kept as small as possible. Ideally there will be five key people; the person in charge of operations, the technical person, the legal person, the business person, and the disinformation person.

The Co-Ordinator:-

The most important person in the operation is the co-ordinator. He is the sole link between the operation and the company. There is no contact between the company and the operatives. This is to protect the company and the people involved.

The project co-ordinator must have a working knowledge of all the fields. Ideally his background will be technical as most of the operation is based on technical countermeasures. A project co-ordinator with a business background will often fail to appreciate the technical avenues available.

The question of loyalty is an important one in this case. If the co-ordinator is good, he will see the prospects in piracy and as such he may be a risk. How can his loyalty be ensured? The most logical method of ensuring his loyalty is to pay his fee in shares in the company and in cash. In this way he will have a vested interest in the success of the operation. It should not be possible to convert the shares for a number of years. The shares would be issued to a front company based offshore. Ideally the company would be based in a country where there is no obligation to disclose the ownership.

The company will only have contact with the operation through the co-ordinator. No written records of these meetings will be kept. The lack of records will help to disguise the company's involvement with the operation. Only the chairman of the board or the managing director would know of the operation.

The co-ordinator selects the people who will control the various aspects of the operation without the help of the company. These people will probably have worked on other projects with the co-ordinator and thus their loyalties will be known. It should be said that their loyalty is to the co-ordinator and the team rather than to the contracting company.

Sometimes a counter piracy operation will be run through a consultancy. This of course would be no ordinary consultancy. It would be the co-ordinator's consultancy and he would contract the other members of the team. In this manner there would be no direct link other than the co-ordinator.

The Technical Operative:-

The technical operative is responsible for the reverse engineering of the pirate descramblers. Ideally he will be a professional revenger, (reverse engineer), with at least three years of experience. It is not a job for a fresh faced university graduate.

Experience in descrambler design is also necessary. The technical operative will design the clone descrambler that will be infiltrated into the pirate market. He will also revenge the pirate descramblers and produce a genuine fake copy. This genuine fake will be designed to begin malfunctioning after a preset time. It will be identical to the pirate descrambler in virtually every respect.

The Lawyer:-

This is the one aspect of the counter piracy operation that will be overtly employed by the contracting company. The lawyer's instructions will come from the counter piracy team.

The lawyer will have no direct contact with or even knowledge of the group. The main reason for this is to protect the group. The group will have to trust each other. Most, if not all, members of the group will have been hackers and as such would find it difficult to trust somebody who does not take the same risks. If the operation went bad, the lawyer would be first to break and collaborate. He would give away the identities of the other members in order to save his own neck. This would naturally seal his fate.

Lawyers have a respect for the law and a faith in the law that would seem to be pseudo-religious. The hackers do not share such faith and as a result the channels lose. The lawyers get rich in the meantime as their fees have to be paid.

In conversations I have had with lawyers, there is one common attribute that I have noticed. They all believed that they could crucify the hacker with legal actions. There is a slightly fatal flaw in their logic. If they were dealing with an ordinary foe they would have a chance of success. It takes considerable mindpower to be a lawyer - it takes a hell of a lot more to be a professional hacker. A lawyer when faced with a hacker will use the instruments of law. A hacker can use a range of options such as; computer viruses, computer record sabotage, ELF zapping the human target. A lawyer who goes after a hacker uninstructed by a counter piracy team is about as much use to a channel as a pair of sunglasses in a supernova. This point was made painfully clear to Sky and News Datacom in Ireland.

The difference between hackers and lawyers is in the mode of thought. Lawyers are used to using critical thinking as opposed to creative thinking. Hackers, while being able to use critical thinking, prefer creative thinking. In the United States, there is one lawyer for approximately every four hundred people. In Japan, there is one lawyer for approximately every nine thousand people. Of course there are the odd few lawyers who do use creative thinking with very good results.

In a counter-piracy operation, the target is a hacker or a commercial pirate who operates extra-legally and as such does not share the lawyer's respect for the law. When you are dealing with an extra-legal operator, you sometimes have to use extra-legal techniques.

The Business Operative:-

The business operative must have experience of setting up and running mail order operations. He must also have a sound knowledge of the black box market. He must have sufficiently low profile as to be virtually unrecognised by the various pirate companies. The finance aspect of the operation will also be covered by the business operative. This implies that he must be adept in setting up offshore companies to run the various operations.

The project relies on the ability of the business operative to cover the trail by using a series of trading companies. These companies will be offshore. The non-disclosure aspects of the companies registration regulations will be used in order to confound anyone trying to track down the operation. The profits if any will be disposed of through this chain of companies.

The Disinformation And Infiltration Operative:-

The final operative is the disinformation and infiltration operative. Of all the operatives, this one is most like the spy. It is his job to plant misleading information about the scrambling system in use.

He must also be prepared to discredit the pirate descramblers and or the pirate companies. A knowledge of usable contacts in the media is essential for this operative. The disinformation has to be diffused through these contacts.

The disinformation and infiltration operative must know how to cultivate contacts and to shape their thought processes. Given the unpredictability of the average person, this would seem difficult. The easiest person to lead astray in this respect is the self proclaimed expert. The writings of these people can easily be identified by the lack of detailed technical data. The non-tech magazines are infested with such writings. By feeding these people with what appears to be some really good information from an "inside source", the mass market can be manipulated into drawing the wrong conclusion.

There is one person that the disinformation and infiltration operative will have to be very careful of; the professional hacker. The professional hacker can, generally, deduce the weaknesses and strengths of a system from a few key facts. The disinformation and infiltration operative will have to protect the client from professional hackers but this may prove impossible. For example see the Filmnet case study.

The flow of information from the company must also be monitored. This task will be covered by the disinformation and infiltration operative. The simplest way to go about this is to see how easy it is to get in contact with the company people responsible for the security of the system. Once contact with these people has been achieved, the ease with which they can be "pumped" for information will be examined. The commonest cover for this kind of information acquisition is that of the technical journalist. The publication for which the journalist is writing need not be mentioned. Free-lance is generally the best cover but if the contact presses for some past article information, the names of obscure signal security publications or even imaginary publications are mentioned. The signal security publication tends to work as the contact will be too embarrassed to say that he is not on the mailing list of such a prestigious publication.

The higher up the contact, the bigger the ego. Such a person will always boast about the system or the power at his disposal. If the person has worked his way to the position, the ego tripping will be greater. There is a common expression among salesmen that the self made man is the easiest customer. He is also the easiest to get information from and as such may be a risk. This risk can be reduced by properly briefing him on what not to say. In many cases, it is better to train his secretary as she is the last line of defence against the hacker trying to acquire information.

Infiltration

In "The Art Of War", Sun Tsu classifies the five types of spy. Local spies, inward spies, converted spies, doomed spies and surviving spies. The local spy would be an inhabitant of the area, people who share the same office building or cleaners for example. The inward spy is an employee of the target company. The converted spy is one of the infiltration operatives of the target company who has been discovered and is willing to work for you. The doomed spy is one who is fed with false information and then infiltrated into the target company. It is known that this operative will desert to the target

company and so can be used to plant false information. The surviving spy is the operative who can infiltrate the target company and come out with the required information without the target company actually suspecting anything. The most valuable spy of all is the spy who does not know that he or she is a spy.

It will be the responsibility of the disinformation and infiltration operative to get an operative into the pirate company. This rarely takes place as the time scale involved can be as long as a year. It is costly and very dangerous. The operative used for this cannot be used in any other operation as the pirate descrambling business is too small. The actual psychological strain on the operative is considerable. He or she has to be totally credible and have a credible background. Nothing in this background can be overlooked. It is better to have studied in a country other than the country of the target firm. This will make it more difficult for the target firm to run checks.

The main problem is that most of the top people in the European Blackbox Industry know each other. As a result any ready-made "ace hacker" who appears on the scene would be quickly investigated.

The most dangerous choice for the operation is a single operative. That is to say an operative who is unmarried or not involved in a relationship. More than one operation has been blown because the operative concentrated on the attractive secretary rather than the operation. During an operation, every infiltration operative will at some time want to tell somebody what he or she is doing. If the operative is single, that somebody may just be an employee of the target company.

The operative used for the infiltration must know as little as possible. If discovered, he or she must not be able to identify he or she is working for. The best way of ensuring this is by making sure that they do not actually know. The only thing that they should know is the information required, and they should only be advised of that after they are infiltrated. They will be hired by a third or fourth party in order to have no direct link with the group. The disinformation and infiltration operative must be prepared to use and if necessary lose the operative. It is not a game and only those who have never been involved in such operations regard it as such. Disinformation and infiltration operatives are quickly turned into cynics. I have never met an optimistic D/I operative.

Getting The Information Out

There has to be some way for the operative to get the information out. Telephones are too risky. They are too easily bugged and very few people can memorise long numbers. They write them down. Anything that is written down can easily fall into the wrong hands. There is a growing trend for business executives to use cordless phones. It is extremely easy to bug one of these phones. The phone itself is the actual bug. The trendy business executive is broadcasting the secrets of his business deals to anybody who will care to listen with a scanner. There is one give-away sound that will indicate the use of a cordless phone: interference from fluorescent tube lighting. Cellnet phones are great for acquiring information on the competition. A simple scanner will make their secrets available as more than a few people in the UK have learned to their cost and other's profit. If cellnet phones have to be used a strict codeword procedure has to be adhered to.

Even the new GSM cellphones are not secure. The algorithm used was apparently published in the USENET sci.crypt newsgroup. The state security services could also listen in on these phones.

The commonest tactic used for getting the information out is to use a postal method or pass the information in a crowded place such as a train station or an airport. Some readers will be thinking about using pubs or streets to pass information. This are common methods in spy novels are far to risky to use in real time unless the operatives are properly trained. In many pubs there will be police either off duty or plain clothes. An information drop would look too much like the passing of drugs. This would rightly cause the police officer to intervene. On an open street, a drop would look too much like a pickpocket operation and some overzealous citizen could intervene. Luckily, technology has provided some easy answers.

The information will not be in the expected format; the roll of film or the microdot. The operative will have to memorise the necessary information such as circuit diagrams or IC numbers or dealer lists. The spy cameras used in the movies can easily be discovered either by accident or on purpose. They are hard evidence. The operative's mind on the other hand, is too ethereal to be hard evidence.

The now standard use of personal computers has made the transfer of classified data easy. All that the operative will need is a floppy disk. Since the operative will have legitimate access to the data on the target's computer, copying the data will appear to be perfectly normal procedure.

Other less time consuming techniques can be used to obtain the required information. Headhunting is about the commonest. The technical people in the target company have to be identified for this procedure. When the person responsible for the design of the descramblers is identified, he or she will receive a call from an employment agency that is trying to fill a vacancy. The actual job package will be made to sound inviting. The target will be told to go to some hotel where the employment agency is interviewing. There will be enough people there to convince the target that it is a real interview.

The target will be quizzed as to the exact nature of the work in which he or she is involved in. If the offer is enticing enough, the target will give all the information required. Everybody says that they would not be fooled by such a set up and that they would not divulge secrets. Perhaps under normal circumstances, but the target will be selected for vulnerability.

In every company there is a security risk. There is always somebody ready to supply information for a price or because they are in some way displeased with the company. The disinformation and infiltration operative must be able to identify these people and use them.

Some of the techniques used are plainly blackmail by normal standards. Homosexuality, sexual deviancy and drug dependency are all usable weaknesses. In many countries, the first option is not as powerful as it used to be but with the advent of AIDS the old fears are being rekindled. It tends to be more usable in the conservative countries. The disinformation and infiltration operative must under no circumstances begin to feel any pity or sympathy for the target. This generally involves some serious mental gymnastics for a normal person.

Most of the people who work in the disinformation and infiltration area of counter-piracy have intelligence ratings among the top 0.5% of the population. This implies that they can have intellects that could unsettle ordinary people. Indeed this would generally be the rule

rather than the exception throughout their childhood and adolescence. Unless they could successfully camouflage their intelligence they were ostracised and made to feel like freaks. If you are part of a society then it can be difficult to transgress its rules. When you have been ostracised from a society there are no rules to transgress. Why should you feel sorry for a being who, had the situation been placed in the 16th century, would be burning you at a stake. I believe that psychologists call it rationalisation.

A common counter-counter piracy trick is to set up an employee to give false information to the counter piracy program. In this case the disinformation and infiltration operative must verify the information so received.

The techniques used by the disinformation and infiltration operative are tantamount to industrial espionage. Industrial espionage is a relative term. When your firm carries out this kind of operation, it is market research, when the opposition do it to you, it is industrial espionage.

Counter-Piracy Today

From the events that followed the hack on VideoCrypt, it was evident that Sky and News Datacom did not have any real counter-piracy program. In fact it seemed that their operation was run by ordinary people. Perhaps they were lawyers and some security consultancy but they were by no stretch of the imagination counter-pirates. In the terms of the Blackbox Industry they were JAFAs. If they were anything other than JAFAs the 07 hack would not have had the effect that it had.

Other channels seem to be learning from the mistakes of News Datacom and Sky. Though it is believed that they still have not created an adequate counter-piracy program yet, France Telecom are trying to fight the hacks on their EuroCrypt system.

Perhaps the main problem with many channels is that they believe that their own people, specifically their corporate security people, can stop hacking. Hacking and piracy are things that many of these corporate security types have little understanding of. The knowledge and tactics required to limit piracy can only be gained in one way.

Hacking And Reverse Engineering.

In professional hacking, there are two types of contract hacking groups. Contract hacking is somewhat different to working for a pirate. All of the hackers in the group will be free-lance. The objective is to hack a system but the beneficiary of the hack is the difference.

The two types of hacker groups are Tiger Teams and Dragon Teams. The origin of the names is obscure. The "Tiger Team" has definite military origins. The "Dragon Team" origin is purely of hacker origin. The concept is Shao-lin Kung Fu. A master would have the Dragon and Tiger brands on his arms. One thing that always baffles non-hackers are the diverse and sometimes arcane influences of hackers.

Tiger Teams

A Tiger team is a group of hackers employed by the system owners to test the security of the system. The will report their hacks and techniques to the system owners thus allowing the system to be made more secure.

Sometimes the people on Tiger Teams are referred to as "tame hackers". This is a contradiction in terms and the it is commonly used by bizoids. It is extraordinarily rare for a hacker to be in the full-time employ of a company. Most companies function on a nine to five basis. A hacker will be at least six hours out of synch with the standard business day. Professional hackers tend to get up in the afternoon and work until six or seven in the morning.

Dragon Teams

A Dragon team is a channel's worst nightmare. It is a group of hackers whose sole aim is to hack the system. The information on the hack will be used to commercially exploit the hack.

To the average channel employee, such groups do not exist. Their image of a hacker is that portrayed by the movie "Wargames". No self respecting hacker is that dorky. The portrayals in the movie "Sneakers" are a lot closer to reality. In certain respects they are a bit too close.

In some books on hacking, the term "Darkside Hacking" is used to describe this type of hacking when it occurs in a computer environment. In cable and satellite hacking, no such distinction exists. There are no clearly defined black and white issues, only varying shades of grey.

The commonest application of a Dragon team is as an offensive weapon. Where a channel is competing for a market, they may hire a dragon team to attack the opposition channel's scrambling system. One of the quickest ways to kill a channel is to make sure that its scrambling system can be hacked commercially.

If a major pirate descrambler industry is built around the opposition channel's scrambling system then other forces can be brought into play. The film producers can be shown how they are losing royalties due to piracy. They will quickly increase the royalties on the films supplied to the hacked channel. Alternatively they will cut off the film supply to the hacked channel until the piracy problem is solved. If the channel has not got the funds to upgrade its descramblers or go to another system, then it will effectively be out of business as a film channel.

Reverse Engineering

Examining an official decoder can be a tricky affair. Unless the system designer is a complete idiot there is a trap that is triggered when an unauthorised person opens the case. There is a wide range of traps but the favourite of most novice designers is the battery/ram trap. A number of traps will be detailed in this chapter as will the hacker approach to dealing with these decoders.

The commonest protection in official decoders is the removal of IC identification numbers. This is an amateurish protective measure as most hackers can deduce the identity of an IC by observing the inputs and outputs on its pins. The system designer who resorts to this method and relies on this alone is extremely stupid. Sometimes, a descrambler will have one or two custom ICs. This is not as difficult to hack as it first appears. Most of the development work will have been

carried out with discrete circuitry. The hacker has to observe the inputs and outputs on the pins of the ICs and design a circuit to emulate them.

The Official Descrambler Booby Traps

The battery/ram trap is the one of the easiest traps to implement. The trap operates by removing the power supply to a RAM containing essential data when the case is tampered with. The key to the trap is a normally closed microswitch. This switch can be held closed by the case or by a screw. The average hacker can normally defeat this trap with ease. The case is drilled and a small observation mirror with light source is inserted. This enables the switch to be seen and neutralised. One rather dirty variation of this trap was the relay and wire trap. A relay was used in the case. When a hacker inserted the observation mirror, he saw the relay. The contacts appeared closed. They were and they also appeared to be connected to the board. There was also an extremely fine wire placed a fraction of a millimetre from the other set of contacts. When the hacker tried to stop the relay from switching by putting a piece of plastic or whatever in to the relay, the wire was forced on to the other set of contacts. As this wire was connected to the RAM power supply and the contacts to ground, this action removed the supply to the RAM. The system designer who used this was also a hacker!

Another trick used by the system owners is covering the track side of the board in epoxy resin. This can defeat amateur hackers. The professional hacker is rarely defeated by this method. Various techniques are used to remove the resin. These can vary from using a scalpel to using a chemical solution capable of dissolving the resin. Many decoders are shipped with the resin uncured. This makes it extremely easy for the hacker to remove it using a scalpel, though it does require the hacker to begin the operation as soon as possible. Most professional hackers try to avoid the use of chemicals. It can be frustrating to find that you have dissolved the printed circuit board along with the resin! For hardened resin, a device called an "ultrasonic hammer" can be used. This device sends ultrasonic shockwaves through the structure of the resin causing it to turn to powder. There are a few resins that this method will not work on. Encapsulation is not generally used on official descramblers and even

on pirate descramblers it is rare to find it on the track side and on the component side. Most descramblers require some sort of set-up adjustments and as a result, no encapsulation is used.

A common trick when resin is used is to mount some of the components on the resin covered side. This means that their values will be unreadable when the resin cures. With resistors this ploy does not cause any problems but certain types of capacitors can have their identification effectively removed by this method. Ceramic capacitors fare worst in this situation as the capacitor can fragment when any attempt is made to remove the resin using even the slightest force.

Removal of component identification is not as secure as some would expect. When the identification on capacitors is removed, the amateur will tend to give up. The professional will just observe the waveforms and desolder the capacitors. A capacitance meter is then used to check the values. Most engineers and technicians may consider using a substitution box to find the value of the capacitor. No hacker would attempt to do this. Using a substitution box especially in a timing chain can create more problems than it can solve. Careful analysis with an oscilloscope, a multimeter and a capacitance meter is required. There are a number of capacitor types, specifically ceramic types, that can look very like resistors to the inexperienced eye. These capacitors are generally used in high spec equipment. One aspect often overlooked by the manufacturers that remove identification numbers on ICs is the fact that the IC number is sometimes printed on the underside of the IC as well as the top.

Surface mount componentry, (SMC) is now used extensively in official descramblers. In the VideoCrypt descramblers it is essential. If standard componentry was used the VideoCrypt descrambler would be two or three times its present size.

Some pirate manufacturers are also employing surface mount technology. This is not to prevent the reverse engineering of their circuitry but rather to shrink the size of descrambler. It has become fashionable for a descrambler to be a small black box. This use of SMC is naive. Since the descrambler is a pirate descrambler, it is inevitable that the descrambler will have to be upgraded. This means that the nicely designed board and componentry will have to be butchered. The upgrade operation is easier to carry out on a standard componentry board.

Reverse Engineering A Doublesided PCB

The following paragraphs are an examination of the process of reverse engineering a double sided printed circuit board. The techniques described are those most commonly used by professional hackers. The costs involved can be considerable as exact 1:1 photography is necessary for the process.

Reverse engineering a double sided board is not as difficult as it may appear. As the process involves disassembly, two boards are necessary as one has to be kept as a working reference.

The first step in the procedure is to have both sides of the board photographed. The photographs should be as accurate as possible. The services of a professional photographer are generally required for this operation.

The second step is to label each component with an identity number and value if they are known. These are marked on an acetate or polyester film overlay. These sheets can readily be obtained from any office supplies shop as they are used for photocopying. This process is carried out for both sides.

The third step is the most complex. The input and output waveforms and DC levels for all ICs are obtained. From this data it should be possible to identify some of the ICs. The ICs are then removed from the board and tested on a breadboard. This generally clears up any doubts about logic ICs. Analogue ICs are slightly more difficult to identify. After all the ICs are identified, new ICs could be tried in their places: This will confirm their identities. This substitution is optional. All components are then removed from the board.

The fourth stage involves copying the track design. This operation is carried out by overlaying the photograph with an acetate film and tracing the pattern. A red ink is used for one side and a blue ink for the other. This is to enable crossing tracks to be differentiated from connected tracks. If the hacker wishes to duplicate the board design, then master artworks are drawn from these tracings.

The fifth stage is to work out what is connected to what-otherwise known as the circuit diagram. This is perhaps the most difficult step of the whole procedure. If a straight forward copy is all that is required, this step is irrelevant, (as long as all the functions of the various potentiometers and trimmers are known).

The best way to commence this step is to draw the IC packages and the component packages on an acetate overlay. The component side photograph is used for this overlay. The track side pattern overlay, the component side pattern overlay and the component overlay are sandwiched together. The pinouts for each IC are applied and the circuit can be worked out from these. The next stage is to replace the IC and component packages with component symbols. The circuit diagram can then be "cleaned up" for greater legibility.

The connections for each component can be stored on a computer. This will enable a PCB designer program to autoroute the tracks if a new PCB is required. Most of the commercial pirate descramblers do not have computer designed boards. The majority of them have very poorly designed boards. Most of these boards were probably designed by people with very little experience in board design. There is a trend for commercial pirate boards to be computer designed. When a computer package is used to design a board it can be a sign that the designer has not the mindpower to design a printed circuit. This seems to be a growing problem among newly qualified engineers who, in some cases, seem to be little more than Glorified Keyboard Operators, (GKOs). This lack of visio-spatial ability often precludes these GKOs from ever working as revengers.

Through the hole plated boards can cause problems for the unwary. Sometimes the pin of an IC will be soldered on the top track but not on the bottom. All such connections have to be checked out prior to disassembly. Plated through holes add to the cost of the PCB. As a result, most commercial pirates just solder the pin or wire on both tracks.

It has been said that reverse engineering requires skills exceeding those of the average electronic or electrical engineer. The skills required can only be gained in one way - actual hands on experience. Every major company has its reverse engineers or as they are known; "revengers". These revengers scavenge the equipment produced by the competition for new techniques and developments.

The technology used in European pirate satellite television descramblers has evolved rapidly since 1989. At that time, there wasn't a microcontroller to be seen. The circuitry used was almost totally discrete and off the shelf. At present, Field Programmable Logic Arrays, Electrically Erasable Programmable Logic Devices and microcontrollers are commonplace.

Some manufacturers still tend to use Read Only Memory ICs to store the algorithm for descrambling. The identification number will, if it is still visible, not give any indication as to the identity of this IC. This can and does confuse a lot of inexperienced hackers. The simplest way to check this device is to monitor the waveforms on the inputs and outputs of the IC. The IC is then removed from the circuit and is read using a computer. The computer steps through the memory addresses of the IC and reads the data at each location. It is then very simple to duplicate the IC by programming an Erasable Programmable Read Only Memory IC with the data. This method cannot be used to duplicate the function of a custom IC.

With custom ICs, the duplication process is a lot more involved. If a large volume market for the pirate descramblers exists, then the professional hacker will certainly consider the use of a chip stripper. The initial development would have been carried out using discrete circuitry so the hacker would try to duplicate the function of the circuit. This can take a few months of development time at best.

The Blackbox Industry is now so large that it is feasible to have a microcontroller or indeed an ASIC completely reverse engineered in the Far East. Indeed it is often unnecessary to have the contents of a microcontroller popped in Taiwan. It can be carried out very effectively due to a flaw in the chip design.

Popping The Chips

The process of extracting the ROM contents of a protected microcontroller is known as “Popping”. In most cases this involves popping the plastic off the top of the chip’s silicon die. Other chips such as certain EPROM types do not require the same type of attention.

The most obvious flaw in security appeared in certain EPROM type microcontrollers. It was possible to reset the protection fuse and read out the EPROM contents.

The problem lay in the design layout of the chip. The protection fuse was not in the same general location as the rest of the EPROM. Therefore if the fuse could be identified, the main EPROM would be covered with a mask. Then UV light would be use to reset the protection fuse.

As it turned out this problem was not limited to the EPROM versions of these microcontrollers. The One Time Programmable versions were actually EPROM versions but without the window. By splitting the chip's plastic it was possible to carry out the same reset operation.

Other chips that were believed to be secure have been popped as a matter of course. The commonest chips at present in the European Blackbox Industry are the PIC16C57 and PIC16C84. The PIC16C57 is an EPROM type and the other is an EEPROM type. The programs have been extracted from each of these chips. This accounts for the similarity between the hacker programs for decrypting VideoCrypt and EuroCrypt.

The designers of scrambling systems often relied heavily on mask ROMmed microcontrollers in their decoder. This has certainly been the case with VideoCrypt. Perhaps as a direct result of their naievete the hackers were able to understand the systems well enough to hack them.

The only things that appear to be in anyway secure are ASICs. Even these can, with the necessary expertise, time and finances, be reversed. However the time frame involved may protect them from casual hacking.

Most of the techniques used in the past by the decoder manufacturers have fallen into disuse. The decoders are readily accessible and of course easily repairable. The circuitry is generally not protected with any booby traps. Of course there is still the odd design from the early eighties that has a lithium battery placed over a RAM chip but these are getting to be very rare.

Perhaps it may well have been a false dawn for the decoder designers. The microcontrollers used in their decoders were mainly secure at the time they designed the systems. It is difficult to avoid the fact that many of them completely underestimated the lengths that would be gone to to hack their systems. In this false sense of security they made mistakes.

The defence of the decoder being a dumb terminal does not hold up well today. The more a hacker knows about a system, the more likely it is that he will come up with a hack.

Grey Market Piracy

Grey Market Piracy is a form of piracy where the subscription for a pay channel is taken out in one copyright area and the decoder or the smart card is then shipped outside the copyright area for use by a third party.

Most of the subscriber agreements have clauses stating that the card or decoder is not to be used outside the copyright area but this seems to have little effect.

The channels are not technically losing any money as the fees are paid in full and indeed these fees are more reliable than some. The main loss for the channels would occur if the Grey Market subscribers stopped their subscriptions.

Like some niggling little itch that you just can't reach, there is the question of lawyers. The basic fact is that when the card or decoder is sent outside the copyright area for use it is illegal in the copyright area that it is not in.

The contract between the subscriber and the channel is null and void. Since one of the parties, the subscriber, entered into the contract on a fraudulent basis, the contract is not valid.

Where the channel can be affected most by the problem is the cost of the programming. In a situation where there is considerable piracy, then the programme providers will set higher fees for the channel.

It would be safe to say that the Grey Market Piracy is the greatest threat facing the channels at the moment. It has caused, in the words of one hacker, the security departments of certain channels to run about acting like headless chickens.

In 1990 and 1991, the subject of Grey Market Piracy was brought to Sky's attention. The press was filled with reports of Customs and Excise aided decoder seizures. These were supposed to have been perceived as victories where in reality they were merely symptoms.

On the surface the demand in Europe for the decoders was for the Sky Sports channel. Of course there is no such thing as partially pregnant. The logical step for the European Sky decoder user was to obtain a Sky Movies smart card.

There was a growing trade in Sky Movies smart cards. At first the whole business was very much under the counter with nothing much being said. Then the pirates got more adventurous and advertise-

ments started to appear in the satellite television press. The subscription would be taken out in the UK or Ireland, (where the services are available legitimately), and the card would then be posted on to the actual user elsewhere in Europe. The problem until recently was strictly one way. Sky would get the subscription and the user would get the card. There would of course be the commission of about eighty pounds for the transaction. This brought the cost of the card to the user to about two hundred pounds or so.

The move to D2-MAC Eurocrypt by FilmNet was meant to reduce piracy. In a sense it did but it also made piracy pay both for the pirate and the channel. This situation changed drastically after the hack.

The advent of D2-MAC EuroCrypt systems means that there are more smart cards around. These smart cards are for FilmNet and TV1000. The rate of exchange was one Sky card for one FilmNet card but the TV1000 card required an extra cash payment. The reason being that the porn on TV1000 is of a more explicit nature.

The channels were benefiting from the whole situation in that they were getting increased subscriptions and the users were getting what they wanted. There were rumours that certain companies were about to lose their Authorised Sky Agent status as a result of Grey Market activity. These rumours turned out to have some element of truth as some time later, the ASA status of Coppull Satellite Television was revoked so they could not sell the Sky Quick Start cards. This was a counter-productive move as Coppull had been selling more than a few subscriptions for Sky. It would appear what Sky tried to create was an example. It backfired and created a hardened animosity in the dealer network.

The problem of knowing where to look was soon solved as the satellite television press filled up with advertisements from companies offering to either exchange Sky smart cards for FilmNet cards or TV1000 cards. In many advertisements, it was simply a case of purchasing the card.

Sky took action against the advertisers though it appeared to be more rational persuasion than anything else. The main perpetrator in the scene is the Sky subscriber who trades the card. While the advertiser is essentially aiding and abetting, he is not directly defrauding Sky. It is a tricky problem that has yet to be resolved.

Most of the channels see Grey Market Piracy as a liability. The reality is that the Grey Market Piracy a channel suffers can bring in cash. This means that they are plainly a revenue source. If and when Europe becomes a single copyright area, Grey Market Pirates would be able to hand over massive audiences. With this in mind, it would be logical for the channels to start negotiating with the pirates so that the market can be controlled. The alternative is widespread small time operations that will only waste time and cost more than they will bring in for the channels.

With FilmNet's use of D2-MAC EuroCrypt, Grey Market piracy has grown in the UK. Before this event, the flow of smart cards was essentially one way. Sky smart cards were going out of the UK and money was flowing back. The trade in TV1000 cards added to this traffic.

Most of the problems with piracy on the systems in Europe would have been drastically reduced had there been some form of active support for Grey Market Piracy from the channels. Most channels did turn a blind eye but there were one or two who stupidly threatened to switch off any traded cards. It is very difficult to look on these channels with mercy.

With the recent hacks on VideoCrypt and EuroCrypt, Grey Market Piracy became a moot point. The piracy quickly turned black.

There was more money in selling pirate smart cards. The Grey Market all but disappeared. Perhaps if the people running the channels had cultivated the Grey Market the effect of the hacks would not have been as great. Of course the corporate lawyers would object but then they do not generally have a working knowledge of how satellite television works. They have become more of a liability to their channels than many pirates.

The Irish High Court Battle

In what is now looked upon as a rather desperate act, Sky tried to pursue David Lyons of Satellite Decoding Systems through the Irish courts. Essentially Sky were claiming that the copyright of the software in their Sky smart card had been infringed.

An Irish court granted Sky an Anton Pilar order which allowed them to enter Satellite Decoding Systems' Offaly trading address and seize items or assets that they believed were directly related to the alleged breach of copyright.

The Anton Pilar order was executed on Friday,December 10th. Apparently David Lyons was not present at the Offaly address when the people from Sky's legal representation called. The strange thing was that Mr Lyons was in transit from the UK via a Ryanair flight when the order was executed. It could have been sheer coincidence.

Sky was intent on getting their hands on the addresses and identities of people who had purchased the PIC cards from Satellite Decoding Systems. This was not to be as Satellite Decoding Systems did not maintain such records. They had instead opted for a monies received form of accounting where customers would be issued with an invoice that would be the only proof of purchase. When the cards were to be upgraded a copy of the invoice had to be returned with the card. In this way the paperwork was to be kept at a bare minimum.

However Sky did not leave empty handed. They seized a number of the PIC cards. The cards seized were the old PIC16C54 types. When Sky implemented an ECM, the PIC cards had to be upgraded. The PIC16C54 is the one time programmable version and as such was not upgradable.

On Thursday December 16th, Sky had to stand before the High Court of Ireland and explain their actions. Actually it appeared that only their legal people were there. Their allegations of copyright infringement were not dealt with at that sitting. Sky's legal team were unprepared. It appears that they are not avid readers of Sun Tzu's "The Art Of War".

Satellite Decoding Systems' legal team had served Sky's legal team with affidavits that clearly nuked Sky's allegations. The case was to be heard at 10:30. Since the papers were served only twenty minutes earlier Sky's counsel had to ask for time to read them and if

necessary reply. Some tooing and froing ensued as they all tried to figure out what time was good for them all. Four o'clock seemed to be a good figure.

The case didn't resume until twenty minutes past four. Sky's counsel did most of the talking. Sky wanted to make sure that Satellite Decoding Systems could not do anything in the meantime. Sky of course would respond to the affidavits but they had to produce them before close of business on Friday.

On Monday 20th December, the case was to resume. Initially it was to be heard in the morning but due to it being the second last day of the legal term, it was necessary to put the case back until four o'clock that afternoon. When the case actually resumed it was closer to twenty minutes past four. The judge, Mr. Justice Keane, stated that the case would be heard on the 21st by another judge as there was insufficient time.

The case was to go before Mr. Justice Flood at eleven o'clock. Eleven o'clock turned out to be a ballpark figure. As it was the last day of the legal term, the pace was hectic. A blizzard of barristers in black gowns and wigs gave the proceedings an aura of a cheap movie about the French Revolution. The question was who was for the Guillotine? Eventually the hearing started. Sky's counsel outlined their position going through the affidavits and the history of events.

The case was complex. News Datacom were apparently satisfied that there were no internal leaks. They also had changed their stance. Now they were claiming that the copyright of their algorithm was breached.

They quoted the affidavit of Ariel Hershler of News Datacom. He claimed that they had developed a "One Way Function". This of course was completely refuted by the affidavit of Doctor Michael Scott of Dublin City University. Apparently Doctor Scott also pointed out that there were numerous mathematical references to the fact that One Way Functions were unproven and therefore Hershler was mistaken in his belief.

Some of Hershler's affidavit, especially the section where News Datacom in Israel tested the PIC cards sounded distinctly unscientific. They put an official card into a decoder. The signal was decoded. Then they put the PIC card into the same decoder and it decoded the signal. From this Hershler believed that it was a copy of the card or a

partial copy. Of course to be fair to Hershler, he probably had to explain the process to some lawyers without the aid of technical terms or analogies. As a result something was lost in the translation.

Strangely the one person of standing who could have commented, Professor Adi Shamir, did not. After all it was Professor Shamir who had allegedly designed the algorithms at the heart of the VideoCrypt system.

The counsel for David Lyons suggested that the suppliers of David Lyons, Megasat in Germany, were willing to disclose their software and algorithms for comparison if Sky would do the same. The judge considered this a good thing. The disclosures will be made in strict confidence to a neutral expert to be agreed by both parties. The expert would then write a report in plain English. The move took Sky's counsel completely by surprise.

This report was to be ready by the 11th of January when the case would resume. The judge did not grant Sky a restraining injunction. David Lyons was now legally able to sell PIC cards with the proviso that he could fully account for the stocks, sales. He also had to keep a record of the identities and addresses of customers. Actually he went off to Disneyland on a Christmas holiday.

The Decision

Like a prolonged death scene in a particularly bad movie, the case dragged on over two months. Sky and News Datacom were unprepared for the decision when it came.

They had lost the case. Furthermore they had lost through their own reluctance and stupidity.

The case resumed in the High Court on January 12th, Sky's counsel pressed their rather fragile case a bit too hard. The idea of the disclosure of source codes and algorithms, in confidentiality, to an independent expert was disliked by Sky. It was almost as if Sky had something to hide.

They even said that the act of transforming the algorithm into source code and programming it into a card was a highly complex task requiring the services of a number of specialists. Often, in the Blackbox industry a design is implemented by one designer. One

designer will code up the algorithm, test the program in an emulator and then blow a few pre-production chips. Perhaps News Datacom and Sky should employ some Blackbox industry designers.

The judge, Mr Justice Flood, was getting irritated. Sky had not agreed to disclose but David Lyons had. Sky perhaps made a serious mistake. Their counsel reiterated how rich an organisation Sky was. Even if the eventual trial went against Sky they could still pay any damages and costs. It looked like Sky were trying to buy the interlocutory injunction. The judge was not impressed. He adjourned the hearing until Friday 14th of January when he would give his decision on the interlocutory injunction.

On Friday, what was meant to be a simple delivery of a decision turned into a yet another long drawn out affair. Sky's counsel wanted to introduce more affidavits but the judge decided not to allow them to be entered. Of course Sky and News Datacom still would not agree to disclose to an independent expert. Finally the judge decided that he would give a written decision on Thursday 20th of January. At this stage the case had been dragged out over two months.

On Thursday 20th of January, the judge read the decision. The decision came as some what of a shock to Sky's counsel. Their application for an interlocutory injunction was dismissed. David Lyons and Satellite Decoding Systems was now free to sell the PIC cards in Ireland.

The reluctance of Sky to disclose their codes played a pivotal role in the decision. David Lyons and his suppliers, Megasat, had offered to confidentially disclose their software. No such disclosure was forthcoming from Sky.

The evidence that Sky had produced was in the form of affidavits that said little. In fact they produced so much paperwork that images of forests being demolished sprung to mind.

The most important mistake that Sky and News Datacom had made was failing to differentiate between the computer program and the results. This point was made clear in the decision as a number of cases that demonstrated precedent were mentioned.

Ramifications

The ramifications of the decision are profound. This Irish Court Decision can now be used as precedence throughout the European Community.

If any channel wants to take legal action against someone who they consider to have infringed the copyright of their system then they will have to disclose.

The disclosure and comparison of software would have to be undertaken in confidentiality. It would most certainly not be a case of entering the details and source code into court records. That would a breach of what arguably could be called trade secrets.

Most algorithms are perhaps trade secrets. But the problem is that the algorithm is not necessarily unique. What Sky and News Datacom appeared to be trying to say was that their algorithm was indeed unique and there was no other way other than copying that someone could come up with an alternative algorithm.

This is a very dangerous position. It precludes all future mathematical and cryptological theory. I doubt very much that Professor Shamir or Ariel Hershler were even consulted on this stance. It sounds like the argument of someone ignorant of cryptology. I guess that Sky and News Datacom let the lawyers handle everything. In this manner Sky and News Datacom joined the gallery of people who believed in an unbreakable code.

History is full of the disasters caused by these people. The outcome of the Battle Of Midway in World War Two was due mainly to the fact that the Americans had cracked the Japanese codes. Most of the major European battles of that war must also be re-evaluated in the light of information that many of the German Enigma codes were cracked.

It is difficult to consider that it would be possible to implement a totally secure and unbreakable code or algorithm. Most of the mathematicians involved in cryptology publish papers in journals or indeed write books on the subject. It would therefore not be improbable that their published papers and books reflect a lot of their thinking on the subject of cryptology. Therefore it may well be possible to gauge how they think in terms of constructing their algorithms.

So from open sources it would be possible to put together a number of possible approaches for algorithms. It is difficult to see how an open source document such as a book or article can be considered a trade secret.

Algorithms are not copyrightable under European law. There was an attempt to try and have the algorithms used in the VideoCrypt system declared part of the design materials. Under European computer law these materials would be protected. The court rejected this argument. An algorithm essentially is a stand-alone unit. The copyright lies in the expression of the algorithm. The expression is the computer program.

The outcome of the case appears to be that any company or channel had better make sure that their crypto systems are very good. The days of relying on 90% bluff and 10% technology are gone. Sky and News Datacom's VideoCrypt is only the first major casualty.

Defences And Rationalisations

When the decision was given by Mr Justice Flood, many of the UK magazines went off with their own versions of what had happened. Most of these articles were not based on any hard data and were mere padding. In fact some of them had quotes from lawyers in the UK who had not apparently read the decision. Given the magazines involved this was par for the course.

The stupidest argument for Sky's position was that the pirate cards had the look and feel of Sky's own card. Obviously the person who came up with this one never actually saw a pirate card. The operation of the pirate cards is transparent. There is no look and feel unless you are rather strangely inclined and are watching a specific non BSkyB channel.

Given the way that the case went, Sky and News Datacom should logically have disclosed in confidence. It was their only option. By refusing to do this, they only made a bad situation worse.

Then the chain of command in the case was poorly structured. The only people representing Sky and News Datacom in the court were their legal team. There was no co-ordinator. The situation was not simulated in a "wargame". As a result there was nobody really in control who could have prevented the disaster.

If it is possible to prove that the hacker created the hack without access to the algorithms or programs in the decoder or smart card, then he can exploit that hack. This is the core message of the decision. Of course there are qualifiers such as the legality of hacking a channel uplinked in the same jurisdiction.

This defence is known as the "Clean Room" defence. Basically the hackers create the hack in an environment devoid of information on the algorithms and programs used by the system under attack. The card is considered as a black box which has an input and an output. The hackers try to emulate the program in this black box without actually directly copying it.

Therefore a cryptological attack on a system that yields a new algorithm could be considered to be a legally valid hack. Of course if the channel has used a published algorithm in their system, then the hackers could claim that the information that they used is in the public domain and therefore not a trade secret. This area of copyright law is complex and very ambivalent.

The only area of law that could be deployed with certainty is the Broadcast Act of each country. Until there is a reciprocal arrangement between all EC countries to extend protection to channels uplinked from another EC jurisdiction, then the channels are relatively unprotected outside their own jurisdiction. Instead of charging around in other jurisdictions, channels should secure their position in their home market. It is the only jurisdiction where the law would be reliably on their side.

Cracking The Code

This chapter is a basic introduction to cryptology and access control. The field of cryptology is highly specialised and is intensely mathematical. There are essentially two sub-fields; cryptanalysis and cryptography. Cryptanalysis is effectively hacking. Cryptography is the development of code systems.

Access control is the denial of access to unauthorised users. This may seem a rather negative definition but it should be remembered that an access control system is designed with attack in mind. To win, a hacker has to conquer. In order for the cryptosystem to win it only has to survive.

In an ideal world, peace protesters would feel really out of place. Access control is a real world concept. The access control system used on a scrambling system has to be secure from hacking or at least not economical to hack. A good cryptographical system is fundamental.

The aim of this chapter is to give you an insight to the processes involved in the cryptosystems used in scrambling systems. Some of the scrambling systems use very good cryptosystems. Others are not so good as they rely on published specifications. Of course they all are eventually hacked.

The Ho Lee Fook hack on VideoCrypt was perhaps the most embarrassing thing ever to befall Sky and News Datacom. They had for years proclaimed that their system would defeat the hackers. It was such a shame that the hackers never believed them. The full details of the algorithm that the hackers used to hack VideoCrypt is given in this chapter. Of course it is often said that we learn by our own mistakes. In this business, if we are lucky, we learn by the mistakes of others.

Relying on a published specification is potentially fatal. It allows the hackers to develop models of the system under attack. In some cases where a published specification was used, the full implementation was not used. For example EuroCrypt is alleged to use DES with the Initial Permutation and inverse Initial Permutation removed.

Cryptography - The Basics

Encryption And Key Distribution

The procedure by which the original data, referred to as "plaintext" is encrypted and turned into encrypted data or "ciphertext" is called the encryption algorithm or key. The basic formula is shown below.

Plaintext + Key = Ciphertext

The security of an encryption system is dependent on the non-linearity of this algorithm. If there is a visible relationship between the plaintext and the ciphertext then it is highly probable that the system can be hacked. If the relationship is so non-linear that there is no immediately discernible correlation, then the algorithm is substantially more secure.

The concept of encrypting a signal is extremely simple. There are two basic processes, substitution and permutation, that are are generally combined together in order to increase system security.

Substitution is where one element of a signal is replaced by another element. For example, DDSO might become 2456. In this example, the letters have been replaced by numbers. The ASCII codes used on computer is essentially a substitution coding system. Each letter is assigned a number. The numbers can then be stored in the computer in their binary equivalent.

Permutation is where the bits in a system are scrambled or mixed into another order. For example, ABCDEF might be translated to BACDEF. In its basic form, this is the simplest system to break. In each language, certain letters are statistically more likely to occur. In English, the commonest letters are E,T,N,A. Then there are other statistical occurrences such as letter pairs like TH, ST and EE.

When these basic techniques are used together to securely encrypt data streams, the combination is termed a product cipher.

Sometimes one or more fixed blocks of data are encrypted using a product cipher. This application is termed a block product cipher. The Data Encryption Standard, DES, is a block product cipher.

6: Cracking The Code

The function of the key in an encryption algorithm is identical to the function of a key in a lock. The algorithm can be considered as a lock. When turned in one direction, the key locks or encrypts the data, when turned in the other direction, it unlocks or decrypts the data.

The simplest algorithm used is called Scratchpad, although it has many other names. It uses the digital "exclusive or", EXOR, function. When two digital bits are compared in this function, the output is high when only one of the bits is high. If both bits are high or both bits are low, then the output is low.

Encryption Example Using EXOR Function

In this example, the word CAT is encrypted with the word DOG as the key. Using ASCII codes, the letters can be represented by a series of numbers; thus CAT becomes 67, 65, 84 and DOG becomes 68, 79, 71. If these numbers are translated into their binary forms, the EXOR function can be applied:

CAT = Plaintext DOG = Key

CAT	0 1 0 0 0 0 1 1 0 1 0 0 0 0 0 1 0 1 0 0 1 1 0 0
DOG	0 1 0 0 0 1 0 0 0 1 0 0 1 1 1 1 0 1 0 0 0 1 1 1
Output	0 0 0 0 0 1 1 1 0 0 0 0 1 1 1 0 0 0 0 0 1 0 1 1

CAT	67 65 84
DOG	68 79 71
Ciphertext	07 14 11

The key returns the ciphertext to plaintext using the same EXOR function:

Decryption Example Using EXOR Function.

Output	0 0 0 0 0 1 1 1 0 0 0 0 1 1 1 0 0 0 0 0 1 0 1 1
DOG	0 1 0 0 0 1 0 0 0 1 0 0 1 1 1 1 0 1 0 0 0 1 1 1
CAT	0 1 0 0 0 0 1 1 0 1 0 0 0 0 0 1 0 1 0 0 1 1 0 0

As can be seen by comparison, the plaintext is returned by EXORing the ciphertext with the key. The sender and the receiver must be in possession of the key to make the system work. Although this is an exceedingly simple method of encrypting a datastream, in

real world systems the key length is generally very large so the system is more resistant to hacking and secure. A simple EXOR cipher is also very dangerous.

The problem with scrambling systems is that the information being encrypted is not plain English or indeed any other language. It is seed information, channel authorisation data or tiering data. Essentially this kind of data is exactly that - data; a stream of binary or hexadecimal. The crypto algorithms encrypt and decrypt this data.

The following are examples of some crypto algorithms. Many of the scrambling systems on the market do not employ the algorithms straight off the page. Instead they make modifications to the algorithms that complicate things for the potential hacker. In some cases, these modifications are necessary to allow the decoder or smart card to process the data.

The Data Encryption Standard

Over the last few years, the Data Encryption Standard has come in for some intense study. Though originally the algorithm was analysed by academics and defence experts, it was the VideoCipher hack that really brought it to the attention of the hackers.

The first form of DES was created by IBM in 1971. It was named Lucifer and was sold to Lloyds. The algorithm as it then existed was not extremely secure though very few people had the computer power to hack it.

By 1974, the algorithm had been reinforced. The Lucifer algorithm had a 128 bit key. The US National Bureau Of Standards saw a need for a standard encryption algorithm that could be used for non-classified government data. The version submitted to the NBS had the key reduced to 64 bits.

The National Security Agency is the electronic eyes and ears of American defence. While the Central Intelligence Agency deals with the ground truth and analysis operations, the NSA monitors all electronic emissions of interest. A 128 bit key DES algorithm would take longer to hack. The 56 bit key version could be hacked within a few hours. The NSA had advised IBM on the creation of certain elements of the algorithm.

For use as the Data Encryption Standard, the key was weakened and other areas of the algorithm were strengthened. This was necessary so that the NSA could hack the DES if required. This was a natural move for NSA. There are those who would protest at such a manipulation but then they are ignorant of the world of electronic intelligence. It would be the height of stupidity to provide one's enemies with a near unhackable cipher system.

The NBS approved the modified Lucifer algorithm for use as the Data Encryption Standard on 15:06:1977. It was documented in the Federal Information Processing Standards Publication 46, (FIPS PUB 46).

The VideoCipher II scrambling system used the DES as the basis for encrypting its digital audio data. As a direct result, more computer time and mind power was tied up attempting to hack it inside the USA than outside. According to some reports this disturbed the US governement departments. The algorithm was never hacked in the sense that someone came up with a general solution. There have been a number of papers on hacking the DES. However the time frames involved would make the hacks unusable. As in most scrambling system applications the DES key changes monthly , weekly or daily, a hack that produced the correct key in a few months is logically useless unless you have recorded the programme and the datastream.

There are a few methods of implementing the DES. The method that concerns us is the Electronic Code Book mode. This generates ciphertext from a 64 bit plain text block and a 64 bit key. This version is the one most commonly used in scrambling system applications. Often, a cut down version with less rounds than the full specification is used.

There are two basic forms of encryption; permutation and substitution. The permutation form merely changes the position of the bits in the sequence. The bits retain their same value either 1 or 0. In some cases the word transposition is used to describe the technique. The substitution form of encryption actually changes the value of the bits. An encryption scheme using both of these forms is generally referred to as a product cipher. Because the input and output are in blocks of bits, the DES format is referred to as a block product cipher.

Electronic Code Book Mode

Key Generation

The first stage of the DES algorithm is the generation of the keys. These keys are generated from the keyword which is 56 bits wide. The bits 8, 16, 24, 32, 40, 48, 56, and 64 are parity bits and are not used in the key generation procedure. The parity is odd.

The Keyword, less the parity bits is fed into a 1 row by 56 column permutation. The permutation is then split into two smaller 1 row x 28 columns permutations. The top permutation is used as C0 and the lower as D0.

The permutation is referred to in the diagram as PC-1 or permutated choice 1. Bit 57 would be the first bit of C0, bit 49 the second and bit 36 the last. Bit 63 would be the first bit of D0 and bit 4 would be the last.

PC-1
57 49 41 33 25 17 09
01 58 50 42 34 26 18
10 02 59 51 43 35 27
19 11 03 60 52 44 36
63 55 47 39 31 23 15
07 62 54 46 38 30 22
14 06 61 53 45 37 29
21 13 05 28 20 12 04

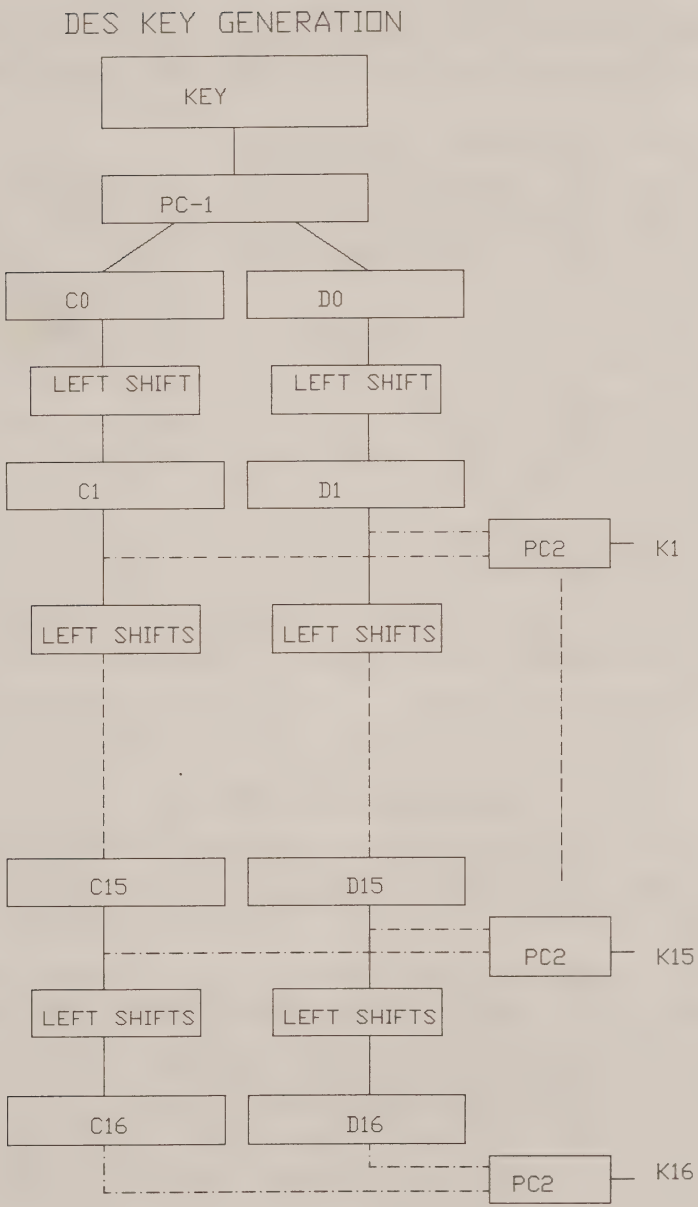
C0
57 49 41 33 25 17 09
01 58 50 42 34 26 18
10 02 59 51 43 35 27
19 11 03 60 52 44 36

D0
63 55 47 39 31 23 15
07 62 54 46 38 30 22
14 06 61 53 45 37 29
21 13 05 28 20 12 04

In order to obtain the keys, the bits of C0 and D0 are left shifted by one or two bits over the procedure. A left shift applied to C0 would result in 57 going to the end. The new first bit would be 49 and the new end bit would be 57.

The number of left shifts to be applied at each step is given in the table below.

Step	Number	Step	Number	Step	Number	Step	Number
01	1	05	2	09	1	13	2
02	1	06	2	10	2	14	2
03	2	07	2	11	2	15	2
04	2	08	2	12	2	16	1


DES KEY GENERATION
KEY
PC-1
C0
D0
LEFT SHIFT
LEFT SHIFT
C1
D1
PC2
K1
LEFT SHIFTS
LEFT SHIFTS
C15
D15
PC2
K15
LEFT SHIFTS
LEFT SHIFTS
C16
D16
PC2
K16

The left shift is a lot less complicated than it sounds. It is also easily implemented in software or in hardware. The left shift function is a common function available in most assembler level languages. The function is also available in some of the higher level languages such as C.

The keys are generated from the blocks by taking each block Cn and Dn and inputting them into the permutation PC-2 or permutated choice 2. This is a 1 row x 48 column permutation. The key length is 48 bits wide.

PC-2

14	17	11	24	01	05
03	28	15	06	21	10
23	19	12	04	26	08
16	07	27	20	13	02
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

The numbers in this permutation refers to the relative position of the bits of the extended block [Cn, Dn]. The first bit of Cn would be the first bit of PC-2. The last bit of Cn would be bit 28 of PC-2. The first bit of block Dn would be bit 29 of PC-2 and the last bit of Dn would be bit 56 of PC-2.

The process of key generation would be fast at machine code level and even faster using dedicated circuitry. It is this element of speed that has led some people to consider that it could be hacked using a parallel attack. Some improvement in the runtime of DES program in a high level language could be obtained by predefining the keys as arrays.

The DES Encryption Routine

The DES encryption routine is a complex and non-linear routine. The reason for this is security. There must be no discernible relationship between the input data or Plaintext and the output data or Ciphertext.

The input block or plaintext is 64 bits wide. The block is first subjected to permutation by insertion into the following 1 row x 64 column permutation designated IP. The permutation is then split into two 32 bit blocks. These are designated L0 and R0. L0 contains the first 32 elements and R0 contains the second 32 elements.

L0	R0
58 50 42 34 26 18 10 02	57 49 41 33 25 17 09 01
60 52 44 36 28 20 12 04	59 51 43 35 27 19 11 03
62 54 46 38 30 22 14 06	61 53 45 37 29 21 13 05
64 56 48 40 32 24 16 08	63 55 47 39 31 23 15 07

The basic step process of the routine can be thought of as a set of modules. Starting with L0 and R0, R0 and the first key, K1 are inserted into the encryption / decryption function module, f. The output of the encryption / decryption function module, f, is EXORed with L0. The output of the EXOR operation provides the new R1 block. The block R0 becomes the new L1 block. This circulation continues as far as L15 and R15.

The blocks L16 and R16 are called the Preoutput. Their sequence is [R16, L16]. R16 is L15 EXORed with the output from the encryption / decryption module function, f. The encryption function module inputs are R15 and K15. The Preoutput block is inserted into the inverse initial permutation.

Initial Permutation	Inverse Initial Permutation
58 50 42 34 26 18 10 02	40 08 48 16 56 24 64 32
60 52 44 36 28 20 12 04	39 07 47 15 55 23 63 31
62 54 46 38 30 22 14 06	38 06 46 14 54 22 62 30
64 56 48 40 32 24 16 08	37 05 45 13 53 21 61 29
57 49 41 33 25 17 09 01	36 04 44 12 52 20 60 28
59 51 43 35 27 19 11 03	35 03 43 11 51 19 59 27
61 53 45 37 29 21 13 05	34 02 42 10 50 18 58 26
63 55 47 39 31 23 15 07	33 01 41 09 49 17 57 25

The inverse initial permutation provides the output block. This block is the Cipher text and is 64 bits wide.

The Encryption/Decryption Function - f

The actual operation of the function module is relatively simple. It appears complex, but it must be remembered that the process is optimised for a computer and not for a human mind.

The R block is 32 bits wide. This block has to be expanded to a 48 bit wide block. The permutation used for this operation is designated the E-Bit Selection Table. The numbers refer to the bit positions in the R block.

The E-Bit Selection Table

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	01

The 48 bit wide block generated from the R block by E is then EXORed with the key to produce a 48 bit wide block. This block is split into eight 6 bit wide sections. These 6 bit wide sections are inputted to eight selection function modules, S1 to S8. These modules select a 4 bit block for the 6 bit input section. These modules are 4 row x 16 column matrices. Since we are dealing with binary numbers, it is necessary to have a row 0 and a column 0.

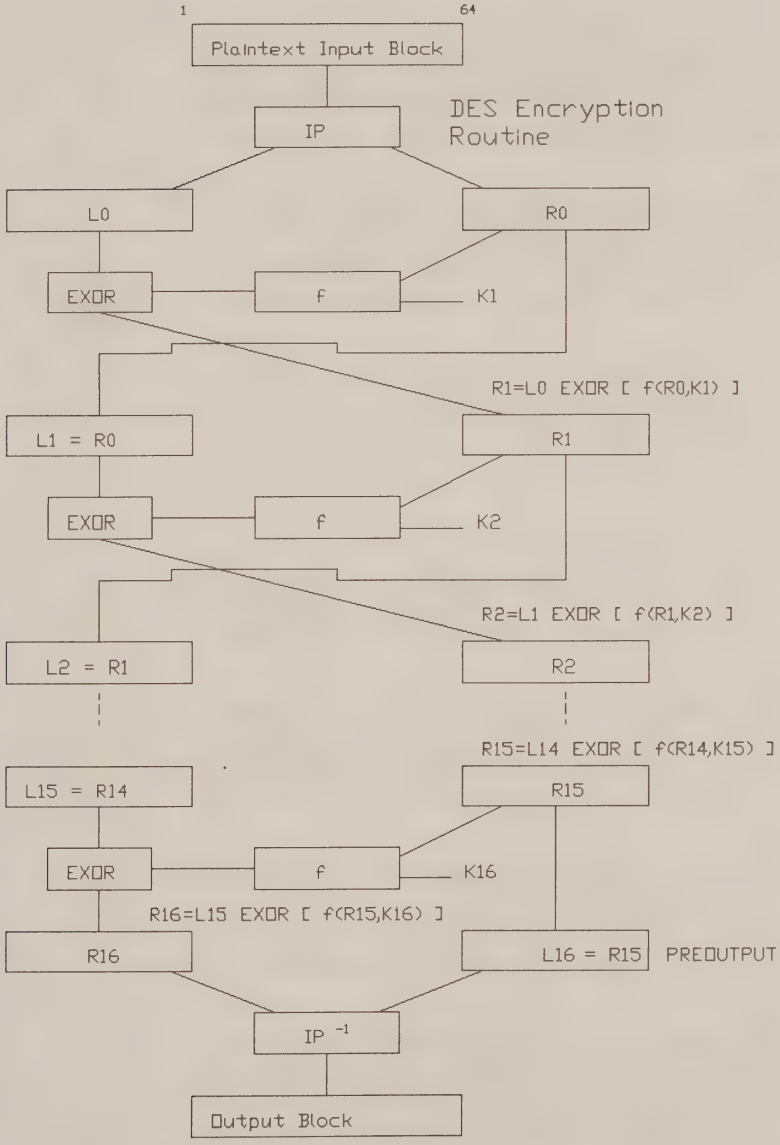
The first and last bits of the 6 bit input section are used to define the row. The possible combinations are 00, 01, 02, 03. These equate to 0, 1, 2, 3 in the decimal base.

The remaining four bits of the 6 bit input section are used to define the column. The range of the bits is from 0000 to 1111 or in decimal base from 0 to 15.

To illustrate the concept, we will use 010111 as the input section for S1. The first and last bits define the row. Therefore the row is 01 or row 1. The remaining bits are 1011 or in decimal, 11. Therefore the column is 11.

The row number is 1 and the column number is 11. By checking the value of the number at this co-ordinate in the S1 permutation, we obtain the four bit number. The value of the number at this location is 11 or in binary, 1011.

This operation is carried out for the eight 6 bit input sections and their respective selection function modules or matrices. The result is a 32 bit wide block.


1
64
Plaintext Input Block
IP
DES Encryption Routine
L0
R0
EXOR
f
K1
R1=L0 EXOR [f(R0,K1)]
L1 = R0
R1
EXOR
f
K2
R2=L1 EXOR [f(R1,K2)]
L2 = R1
R2
R15=L14 EXOR [f(R14,K15)]
L15 = R14
R15
EXOR
f
K16
R16=L15 EXOR [f(R15,K16)]
R16
L16 = R15
PREOUTPUT
IP -1
Output Block

The S-Boxes

S1
14 04 13 01 02 15 11 08 03 10 06 12 05 09 00 07
00 15 07 04 14 02 13 01 10 06 12 11 09 05 03 08
04 01 14 08 13 06 02 11 15 12 09 07 03 10 05 00
15 12 08 02 04 09 01 07 05 11 03 14 10 00 06 13

S2
15 01 08 14 06 11 03 04 09 07 02 13 12 00 05 10
03 13 04 07 15 02 08 14 12 00 01 10 06 09 11 05
00 14 07 11 10 04 13 01 05 08 12 06 09 03 02 15
13 08 10 01 03 15 04 02 11 06 07 12 00 05 14 09

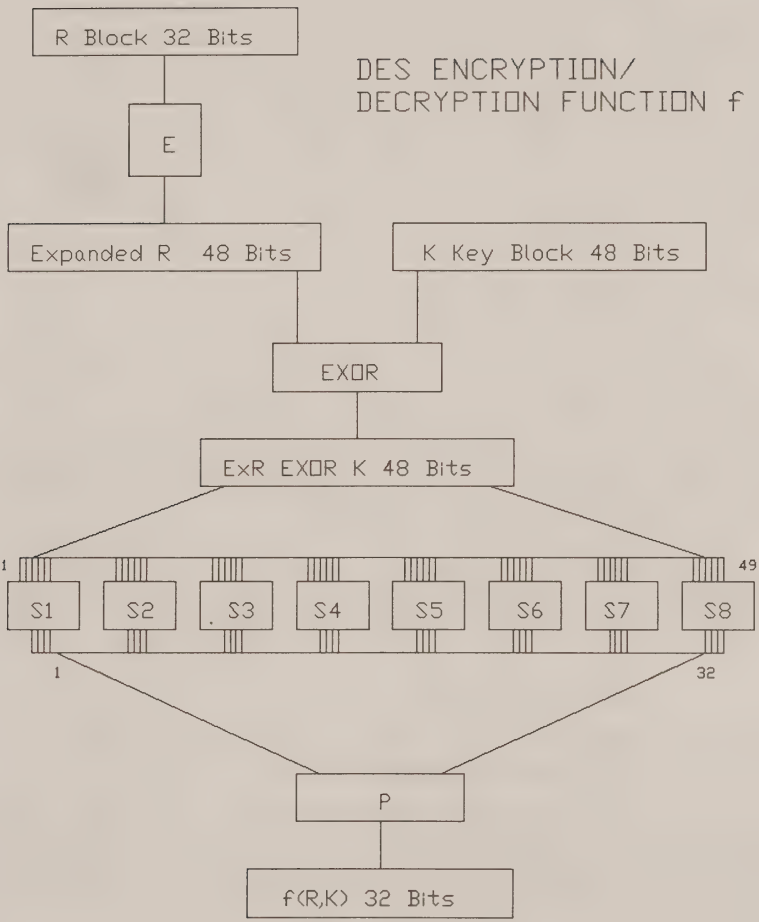
S3
10 00 09 14 06 03 15 05 01 13 12 07 11 04 02 08
13 07 00 09 03 04 06 10 02 08 05 14 12 11 15 01
13 06 04 09 08 15 03 00 11 01 02 12 05 10 14 07
01 10 13 00 06 09 08 07 04 15 14 03 11 05 02 12

S4
07 13 14 03 00 06 09 10 01 02 08 05 11 12 04 15
13 08 11 05 06 15 00 03 04 07 02 12 01 10 14 09
10 06 09 00 12 11 07 13 15 01 03 14 05 02 08 04
03 15 00 06 10 01 13 08 09 04 05 11 12 07 02 14

S5
02 12 04 01 07 10 11 06 08 05 03 15 13 00 14 09
14 11 02 12 04 07 13 01 05 00 15 10 03 09 08 06
04 02 01 11 10 13 07 08 15 09 12 05 06 03 00 14
11 08 12 07 01 14 02 13 06 15 00 09 10 04 05 03

S6
12 01 10 15 09 02 06 08 00 13 03 04 14 07 05 11
10 15 04 02 07 12 09 05 06 01 13 14 00 11 03 08
09 14 15 05 02 08 12 03 07 00 04 10 01 13 11 06
04 03 02 12 09 05 15 10 11 14 01 04 06 00 08 13

S7
04 11 02 14 15 00 08 13 03 12 09 07 05 10 06 01
13 00 11 07 04 09 01 10 14 03 05 12 02 15 08 06
01 04 11 13 12 03 07 14 10 15 06 08 00 05 09 02
06 11 13 08 01 04 10 07 09 05 00 15 14 02 03 12


R Block 32 Bits
DES ENCRYPTION/
DECRYPTION FUNCTION f
E
Expanded R 48 Bits
K Key Block 48 Bits
EXOR
ExR EXOR K 48 Bits
1
49
S1
S2
S3
S4
S5
S6
S7
S8
1
32
P
f(R,K) 32 Bits

S8
13 02 08 04 06 15 11 01 10 09 03 14 05 00 12 07
01 15 13 08 10 03 07 04 12 05 06 11 00 14 09 02
07 11 04 01 09 12 14 02 00 06 10 13 15 03 05 08
02 01 14 07 04 10 08 13 15 12 09 00 03 05 06 11

The 32 bit wide output from the selection modules, S1 to S8, is inputted to the P permutation which is 1 row x 32 columns. The permutation is referred to as the Permutation Function P. The numbers refer to the position of the bits in the 32 bit wide output from the selection modules. The numbers run from left to right.

P Permutation
16 07 20 21
29 12 28 17
01 05 23 26
05 18 31 10
02 08 24 14
32 27 03 09
19 13 30 06
22 11 04 25

DES Decryption Routine

The same algorithm is used for decryption. The key application sequence is reversed. The sixteenth key, K16, is used in the first place or round and the first key, K1, is used in the last round.

There are a number of keys for which another key exists. These keys produce all zeros or ones or an alternating zero one pattern after the first step of the key generation routine.

The other DES modes are Cipher Block Chaining, (CBC); Cipher Feedback, (CFB) and Output Feedback, (OFB). These modes are more secure than the basic Electronic Code Book mode.

Cipher Block Chaining - CBC

The principle behind CBC is simple. Each 64 bit plaintext input block is EXORed with the previous 64 bit ciphertext block.

On the surface it appears straightforward. The problems lie in the beginning block and the fact that each output block is a function of all of the previous blocks. Since the first block has no previous ciphertext block, an initialising variable or block has to be used.

Since all subsequent blocks are functions of the previous blocks, an error in one block will cause errors all of the subsequent blocks. The term for this is “error extension”. On encrypted audio this will show up

as crackling. On encrypted video it shows up as sparklies. On data it requires the complete retransmission of the data. Error checking is carried out on the ciphertext rather than on the plaintext.

Cipher Feedback - CFB

Cipher Feedback mode is used where the plaintext used is continually less than a full 64 bit block. To reach a full block, the plaintext would have to be padded out with random data. Since the number of bits used is less than 64, the technique is commonly referred to as "M bit Cipher Feedback". M is any number between 1 and 64.

In this mode, the input to the DES algorithm is the previous 64 bits of ciphertext. The input to the DES algorithm is held in a shift register that has an initial value at the start of transmission. The M bit plaintext is EXORed with the left most bits of the output of the DES algorithm. The ciphertext produced is then fed back into the shift register.

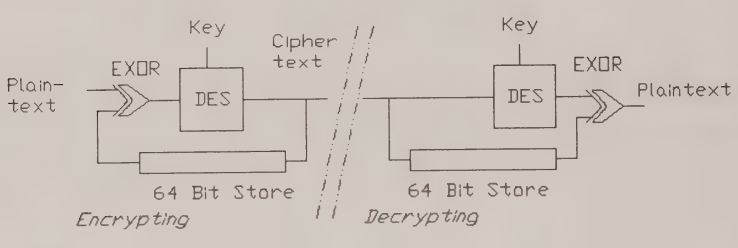
Output Feedback - OFB

Output Feedback mode uses the output of the DES algorithm as the feedback to the DES input shift register. This is referred to as "M Bit Output Feedback". M is any number between 1 and 64. In this mode the output of the DES algorithm is EXORed with the M bit plaintext.

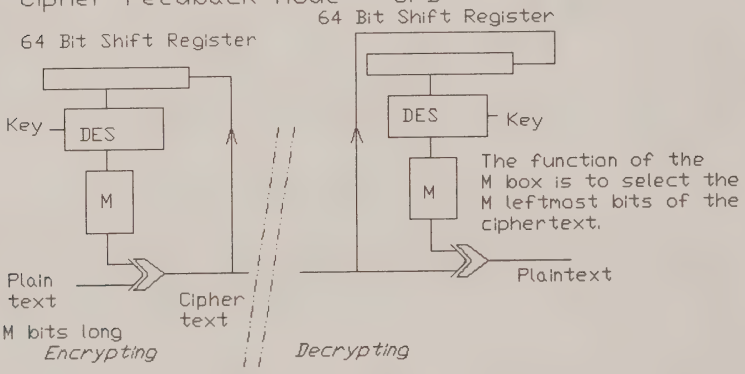
If the receiver and transmitter lose synch then a new initial value must be inputted to the shift register. It is not necessary for the initial values to be encrypted.

DES Encryption Modes

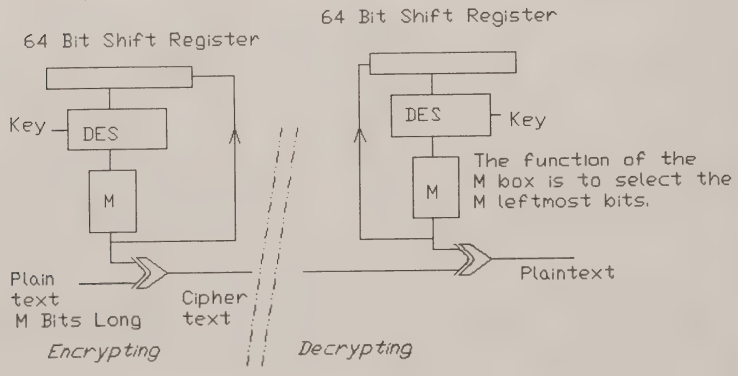
Cipher Block Chaining - CBC



Cipher Feedback Mode - CFB



Output Feedback - OFB



The RSA Algorithm

The RSA algorithm, or to give it its proper title, the Rivest Shamir Adlemann algorithm relies on the difficulty of factoring large numbers. Mathematically it is one of the simplest algorithms. Computationally, it can give a few problems. These problems can be overcome but the algorithm is slow compared to the DES.

The RSA crypto system is a Public Key System. This means that one key is used to encrypt the data and another key is used to decrypt the data. The encryption key is a pair of integers (N,P). The decryption key is the integer pair (N,S). The integer S is kept secret. The integers N and P are published. This is the mathematical definition. From here on I will refer to S as the secret key, P as the public key and N as the address.

Modulo arithmetic is used in the algorithm. For those who have temporarily forgotten how modulo arithmetic works this is a very brief explanation. In the example below, the modulus is the amount left over from the division of the nearest integer multiple of N. Thus if N=5

17 Mod 5 = 2

5 * 3 = 15

17 - 15 = 2

There are four basic elements in the system. The first two elements are prime numbers. (They are only divisible by themselves and one.) These will be called X and Y in the example.

The third and fourth elements are the secret and public keys. The secret key is a prime number. The public key is chosen using the formula below. In the example, the secret key is S and the public key is called P.

The product of the primes X and Y is also published. This is like the telephone number of the user. In the example this product is called N.

X= Prime Number 1 S= Secret Key = Prime

Y= Prime Number 2 P= Public Key

N= X * Y P is chosen so that P * S Mod ((X-1)*(Y-1)) = 1

P= (((X-1)*(Y-1))+1)/S

Encrypting:

ciphertext = (plaintext)^{P} Mod N

Decrypting:

plaintext = (ciphertext)^{S} Mod N

As can be seen from the above, it is simple in theory. To obtain the ciphertext from the plain text, raise the plaintext to the Pth power modulo N. To recover the plaintext from the ciphertext, raise the ciphertext to the Sth power modulo N.

Worked Example Of RSA Algorithm

X= 47 (Prime 1) S= 97 (Secret Key - Prime)

Y= 79 (Prime 2) P= ((47-1)*(79-1))/97 = 37

N= 47*79 = 3713

Plaintext = AT

To convert this into a simple numeric code, each letter of the alphabet is assigned a number from 1 to 26. Therefore AT becomes 120.

Encrypting:

Raise 0120 to the 37th power modulo 3713

ciphertext = 120^{37} Mod 3713

ciphertext = 1404

The method used to raise the plaintext to the 37th power modulo 3713 is known as "Exponentiation By Repeated Squaring And Multiplication". It is a very elegant mathematical short cut. Of course this is not the only algorithm that could have been used in this application.

The "Exponentiation By Repeated Squaring And Multiplication" algorithm is shown below.

H

To obtain M^H Mod N

Step 1: Display H in its binary format. (Hn-H0)

Step 2: Set C=1

C= C^2 = 1C Mod N

C= C^2 = MC Mod N

Note Hn is always 1.

Step 3: Set i=n where n is the number of digits in binary H.

Step 4: Set C= Remainder when C^2 is divided by N

Step 5: If Hi=1 then set C= Remainder when CM is divided by N

Step 6: Decrement i by 1

Step 7: Halt if i=1 else goto step 4

Applying this to the figures in the example gives;

M=120, H=37 and N=3713 Binary H= 100101

Step 1: C=1

C= 120C Mod 3713 = 120 Mod 3713 1

i=6

C= 120^2 Mod 3713 = 3261 Mod 3713 0

i=5

C= 3261^2 Mod 3713 = 89 Mod 3713 0

i=4

C= 89^2 Mod 3713 = 495 Mod 3713

(495 * 120) Mod 3713 = 3705 Mod 3713 1

i=3

C= 3705^2 Mod 3713 = 64 Mod 3713 0

i=2

C= 64^2 Mod 3713 = 383 Mod 3713

(383 * 120) Mod 3713 = 1404 1

i=1

Therefore 120^{37} Mod 3713 = 1404

Decrypting:

To decrypt the ciphertext raise 1404 to the 97th power modulo 3713.

plaintext = 1404^{97} Mod 3713

plaintext = 120

In this case M=1404, H=97 and N=3713 Binary H=1100001

1404C Mod 3713 = 1404 Mod 3713 1

C= 1404^2 Mod 3713 = 3326 Mod 3713

(3326 * 1404) Mod 3713 = 2463 Mod 3713 1

C= 2463^2 Mod 3713 = 3040 Mod 3713 0

C= 3040^2 Mod 3713 = 3656 Mod 3713 0

C= 3656^2 Mod 3713 = 3249 Mod 3713 0

C= 3249^2 Mod 3713 = 3655 Mod 3713 0

C= 3655^2 Mod 3713 = 3364 Mod 3713

(3364 * 1404) Mod 3713 = 120 1

The use of the "Exponentiation By Repeated Squaring And Multiplication" algorithm allows the whole process of implementing the RSA algorithm to be easily computerised. In fact a very simple BASIC program can be written for the implementation.

The main factor in the security of the RSA algorithm is the size of the prime numbers used. These numbers are generally over a hundred digits long. A simple search of low primes would have revealed the values chosen in the example. A computer program to factor the address N would take less than a second. Once the primes X and Y are known, the value of the secret key S can be calculated by rearranging the formula used to obtain the public key P. In this case divide by P rather than S.

Authentication And Verification

Authentication is now essential in crypto systems. The hacker must not be able to substitute his own key for that of somebody else. Conversely he must not be able to use someone else's key in his own decoder. If this occurred he could then read all messages encrypted with that key.

This particular failing led to the downfall of the VideoCipher II system. VideoCipher II was based on a heirarchical key set. A monthly key decoded the session key. The monthly key was transmitted in an encrypted form to each authorised decoder using that decoder's unique key as the encryption key. The monthly key could be decrypted with a valid key. It did not matter that the key used in a descrambler was not the actual descrambler's key but one extracted from another descrambler. This was a disaster for VideoCipher II and it was something that the system never fully recovered from.

Ideally the crypto system should be able to ensure that the receiver can identify the transmitter from the message received or at the very least be able to guarantee that the message is indeed from the sender. In a word the message must be authentic.

This is essentially a signature facility. Another reason for the use of a signature facility is the possibility that someone may interfere with the message. Or to put it in plainer terms, a hacker will try to manipulate the message to make the descrambler operate unofficially.

There are a number of possible systems that can be used to provide the Authentication scheme in a scrambling system. The examples covered are the basic RSA signature and the Fiat Shamir Zero Knowledge Test.

RSA Signature

This signature operation in RSA is relatively simple. The transmitter takes a message and raises it to the power of his Secret Key (S) modulo N.

The receiver then uses the transmitter's Public Key (P) to raise the ciphertext to the Pth power modulo N. The result is the plaintext message.

The message could be a random piece of information or something such as the date or the channel number. There would be no real transfer of knowledge between the transmitter and the receiver.

Transmitter: Published data= N, P

Message = plaintext

Encrypting:

Ciphertext = $plaintext^P$ Mod N

Decrypting:

Receiver: Uses transmitter's N and P values to restore message.

Plaintext = $ciphertext^P$ Mod N

There are of course other methods of signing data. This RSA method is useful where there is a lot of computing power. However for smart card applications, where the eight bit processor still rules, other less cycle consuming algorithms are required.

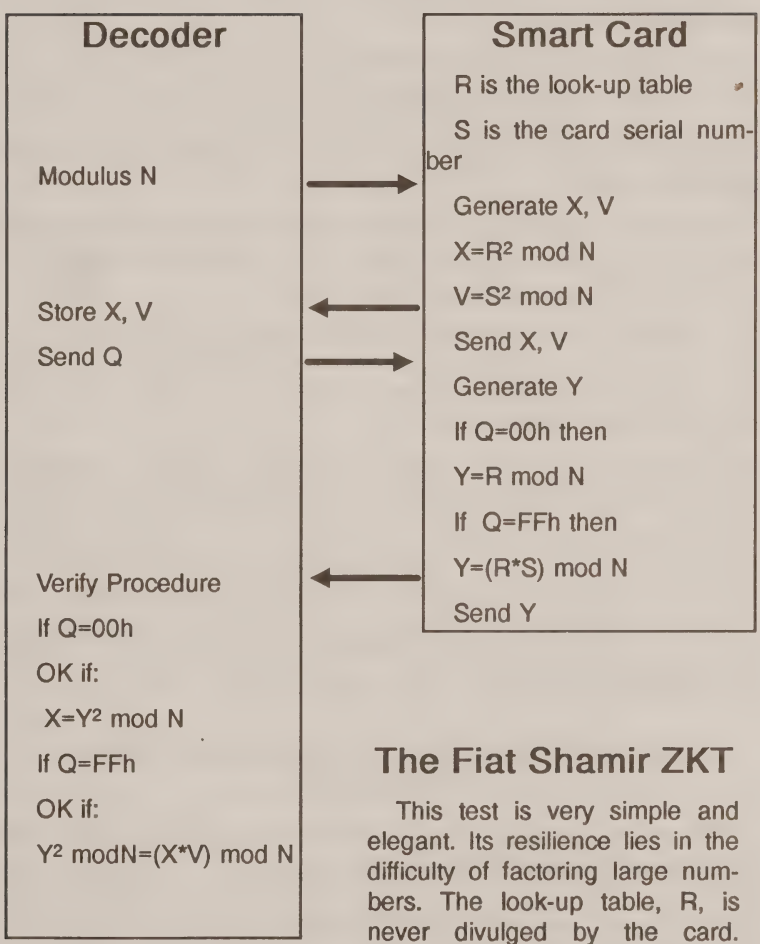
Fiat Shamir Zero Knowledge Test (ZKT)

The Fiat Shamir Zero Knowledge Test is, according to VideoCrypt brochures, used to verify that the packets of information in the VideoCrypt access control system are valid and have not been tampered with.

The problem is that the brochures are less than clear as to where in the VideoCrypt system that the the ZKT is used. From what can be established, it is used in the over the air data packets but not in the actual card - decoder packets.

The original paper on the algorithm was published in the proceedings of Crypto '86. The information outlined here is derived from a paper on an Open Smart Card Interface for D2-MAC. The paper was published in 1991.

The Fiat Shamir algorithm relies on the difficulty of factoring and extracting modulo square roots. Basically the look-up table R is never sent out of the smart card. The card serial number is, theoretically not supposed to be sent outside of the card.



The Fiat Shamir ZKT

This test is very simple and elegant. Its resilience lies in the difficulty of factoring large numbers. The look-up table, R, is never divulged by the card. Therefore the only approach would be to pop the smart card and extract the table.

In the D2-MAC application outlined in the paper, the modulus, N, is a 64 Byte number. This gives effectively 2^513-1 numbers that can be used for the modulus.

The modulus is of course a limiting factor on the size of the look-up table, R. If the modulus is greater than R then the result of R mod N is zero. The fact that R mod N is zero when the look-up table is a multiple of R could be considered as a guideline for a number crunching attack

What the ZKT has in its favour is that the numbers involved are very large. Factoring algorithms are slow and as a result the chances of the look-up table R being discovered are not good.

A potential weakness would be the reduction of the size of the look-up table and modulus. A number of computers working in parallel may just have the chance of producing the look-up table as the result of a guided Brute Force Attack.

The ZKT was just one of the authentication routines mentioned. In this application it was to be used to authenticate the smartcard before the smartcard could proceed to decode the channel. The D2-MAC systems tend to go for a different security approach. Whereas in the VideoCrypt system it is the algorithm that is the most valuable aspect, it is the key tables that are the most valuable in D2-MAC systems. This of course points to the probability that the routines used in D2-MAC EuroCrypt are either DES or a derivative of DES.

Hash Functions and Message Digest Algorithms

A Hash function produces a fixed length output from a block of data. The length of the input can be fixed or variable. The hash output is commonly referred to as the hash value. Essentially the hash function produces what could be called a fingerprint of a block of data. When the function is hard to reverse, it can be referred to as a Message Digest.

Reversing the hash should be extremely difficult. It should not be possible to rebuild the input data from the output. Another factor is that in an application such as smart card usage, the actual algorithm used for the hash should not be known.

The reason for this is that if a single algorithm is used the system can be compromised if the algorithm is discovered. The hash is commonly used to prove that the addressing data and subscriber data is valid and has not been altered.

One Way Functions

A One Way Function is like a religious deity. It depends on faith for its existence. Without faith it is nothing. It does not exist. Of course like every religious deity, One Way Functions have their true believers and disbelievers.

Technically speaking, a One Way Function is a function that is extremely difficult, if not impossible, to reverse. The procedure can only go one way hence the name.

The problem with the One Way Function is that the concept is fundamentally flawed. It rules out any future discovery or theory. It is too reminiscent of that Holy Grail, the unbreakable cipher. Normally when someone invents what they believe to be an unbreakable cipher, someone else is around to crack it.

History is full of such cracked unbreakable ciphers. World War Two was a war where many key events and battles were decided by the intelligence gathered from codebreaking. Indeed there are indications that the attack on Pearl Harbour was expected as the Japanese diplomatic ciphers were being cracked by the Americans and the English.

The One Way Function has to be very difficult if not impossible to reverse. There are a number of methods that can be used to achieve this level of complexity.

The first method is to design very complex algorithm or equation. This approach is fine if there is a lot of processing power in the electronics. This method may be more suited to personal computers or similar applications.

The second method is to use a simple routine a number of times. The routine would be relatively short but the fact that it is repeated so many times would make the reversal extremely difficult. In terms of implementation in a smart card this is the easiest. It is merely a question of setting a loop.

The simplicity and elegance of the second method makes it ideal for implementation in a smart card. The majority of smart cards are still using eight bit processors. They also run at relatively slow clock speeds.

The routine at the core of the One Way Function is perhaps the weakest link. If this routine is not properly designed then the number of times that it is used may be irrelevant. There could be a way of cracking it by comparison.

Theoretically, the bits in the output of the One Way Function should have no visible relationship with each other. This of course would be the theoretical model. In the real world sacrifices to the demons of expediency have to be made. The processor word length is one of these sacrifices.

With eight bit processors, it is possible to have sixteen bit wide registers so the output of the routine could be sixteen bits wide. With the limited RAM available on the smart card, this would be a rather inelegant implementation in terms of memory usage. Using an eight bit output each time would be far more elegant and a lot easier to implement.

In the second method, the routine would be applied a number of times. A typical procedure would be to EXOR the output of the routine with the contents of the output block which in the smart card model would be a single byte.

The output block is effectively the accumulation of all of the previous outputs of the routine. The initial state of the output block is zero. In mathematical terms it would be the modulo 2 sum of all of the routine's outputs.

Unfortunately this model is rather simplistic and is also very vulnerable. The same keys are applied on a repeating basis. This makes the whole chain relatively linear.

The keys K_0 - K_n are selected on a repeating basis. Therefore there is a risk of a pattern developing. The keys would effectively become constants. It should be remembered that any potential cryptanalyst will have a large amount of ciphertext and its corresponding plaintext.

It is therefore a good thing to include as many elements of non-linearity as possible in the model. The first step would be to make the selection of the keys non-linear.

Since the application is smart card based, the memory available for key tables will be limited. By using a look-up routine to select the keys, a virtual key table many time the size of the original can be created. This look-up routine would make the process of cracking a lot harder.

A good example of this type of thinking can be seen in the DES algorithm's key generation routine. The DES algorithm generates sixteen forty-eight bit keys from a single fifty-six bit key. This provides each round of the DES with its own key.

Even when the model is updated, the process is still relatively linear. This chain is repeated for each block of the output. The function f is still uses the inputs from the key table and a known variable, the input data. Since the input data is a known factor, it could be used as a path of attack by any cryptanalyst.

In terms of computer programming the model is very messy. The chain is repeated for every output block. In a situation that requires a multiple block output, for example one eight bytes wide, using a chain for each output block would be wasting processor time. It would also make each output block unique thus multiplying by eight the amount of information available to a cryptanalyst. If the complete number of output blocks formed one single output then things would be a lot more complicated.

Again, the DES algorithm can be used for ideas. In the encryption and decryption rounds, part of the previous round's output is used as the input for the next round. A cipher that uses this procedure is called a Fiestel Cipher. It is an elegant method that increases the complexity of cracking the algorithm. The output of each round is effectively a product of the outputs of all the previous rounds.

By feeding each output block into the function f to generate the next output block would change the program from a simple EXOR equation to a non-linear one.

Many of these ideas about One Way Functions can be seen in the Ho Lee Fook algorithm. This is the algorithm that the hackers used to hack the VideoCrypt system.

PRNGs and PRBSGs

A random number is a number generated at random from a possible set of numbers. There is apparently no chance of anybody predicting the next number that will be selected. That kind of thing is fine for Lottery tickets and such. In signal security, there is a demand for two or more random number generators to work in synch. This is impossible as they would not be generating random numbers. The compromise is a Pseudo Random Number Generator.

A Pseudo Random Number Generator generates a sequence of numbers that appears to be chosen at random. In reality, it generates a sequence of numbers using a mathematical equation. A PRNG relates to a number with a specific maximum number of digits. This would mean that the output of the PRNG would be EXORed with the data on a parallel basis. While it is possible to fabricate PRNGs, it is easier to fabricate a PRBSG.

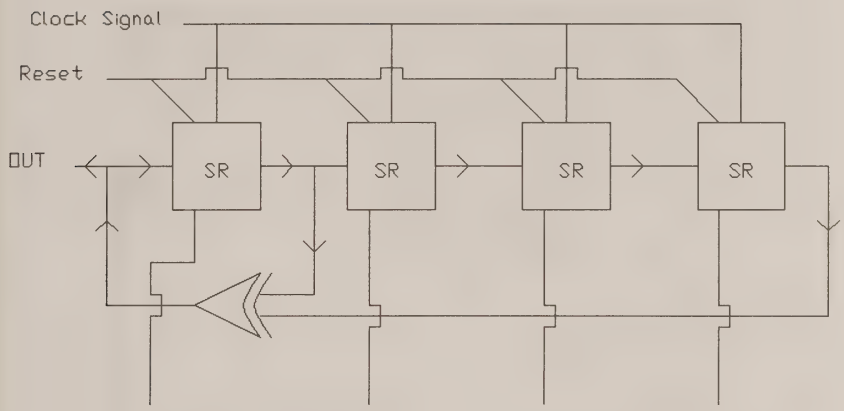
In security applications, a Pseudo Random Binary Sequence Generator is used instead of a PRNG. The PRBSG generates a one bit wide output. This can be EXORed bitwise with the datastream.

In terms of hardware, a PRBSG is easily implemented using some shift registers and an EXOR gate. At start up, the shift registers are filled with a key or seed value. The system clock then shifts the bits through the registers. The inputs to the EXOR gate are called the feedback points.

The datastream produced by EXORing the output of the PRBSG with the data would then be harder to hack. Since the bit can only be one or zero and each bit in the new data stream can be one or zero, the prospective hacker would have to acquire a lot of the ciphertext and a lot of plaintext. Using some complicated statistical analysis and matrix algebra, the properties of the PRBSG may be deduced. These properties would be the length of the shift register and the feedback points of the PRBSG. He would still have to acquire the seed word. This is the data loaded into the shift registers when the PRBSG is initialised. This all assumes that the feedback logic is linear. If it is non-linear, then the task will be almost impossible.

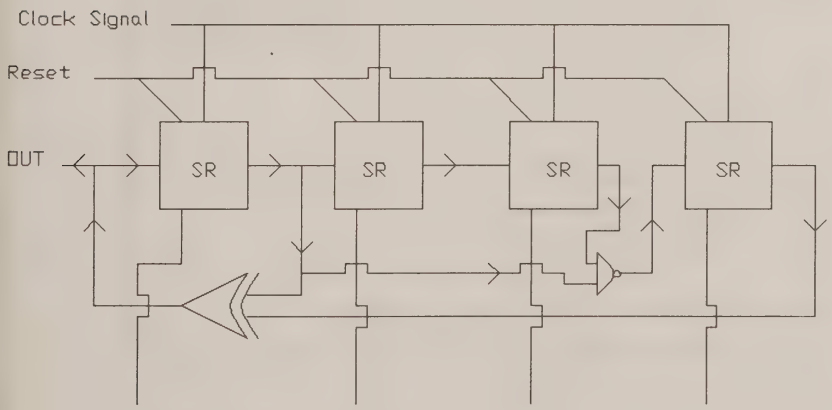
PRBSGs are commonly used in digital audio applications to shape the spectrum of the signal. The use of the PRBSG allows the datastream to appear as random 1s and 0s otherwise known as noise.

PRBSG With Linear Feedback



Seed Word Data. This Data Is Loaded Into The Shift Registers On RESET.

PRBSG With Non-Linear Feedback



Seed Word Data. This Data Is Loaded Into The Shift Registers On RESET.

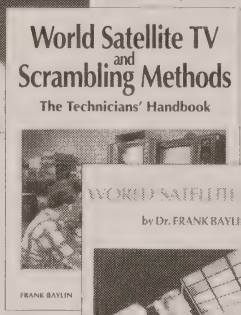
Baylin Publications

ALL ITEMS EX-STOCK.

24 River Gardens, Purley, Reading.
RG8 8BX. England.
Tel/Fax 0734-414468
Mobile 0836-582785

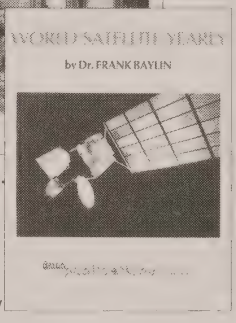
Pay by: UK£ cheque, Access, Mastercard, Visa, C.O.D.

Ku Band Satellite TV, Theory, Installation & Repair 4th Edition. Footprints, dish theory, cables, site survey, polar mount adjustment. ***£25.***



European Scrambling Systems, Circuits, Tactics & Techniques. By John McCormac, digital sound, smart cards, pirate decoders, for hackers. 4th Edn. ***£32.***

World Satellite TV & Scrambling Methods. 3rd Edition, by Baylin, Madox & McCormac for the service engineer. ***£29.***



Home Satellite TV Installation Videotape. Forty minutes VHS Pal. See how 3 metre dishes are installed. ***£27.***

Satellite Installation Guide. 3rd Edition. By John Breeds. ***£15.***

The Satellite Book. 3rd Edition. A complete guide to satellite TV . Theory and practice by John Breeds. ***£32.***

TVRO System Analysis and Aiming Software. 5.25 or 3.5 disk, (DOS 3.2). Calculates dish size and lists coordinates of all satellites in view. ***£39.***

Satellite Toolbox Software, for IBM Comp. Hard Disk– 5.25 or 3.5. ***£59.***

Wireless, Cable & SMATV, Microwave broadcasting & cable TV. ***£35.***

World Satellite Yearly by Dr. Baylin, Loading and 200 Footprints. ***£59.***

PRICES INCLUDE P. & P. UK. Airmail Europe add 10%. Outside Europe + 30%.

The Ho Lee Fook Algorithm

Very few people know exactly when the VideoCrypt smart card was hacked. There are many rumours and claims. Some claim it was all the work of one hacker. Others claim that the smart card itself was reversed. Either way the hack happened and the credibility of Sky and News Datacom was irretrievably shattered.

When that aura of mystique is dispersed, the VideoCrypt system is at once simple and complex. It is simple in that the present 07 implementation dangerously relies on a single layer of authentication. It is complex in that there are a lot of unused aspects. One Irish hacker summed it up in the following manner: "if it was any holier it'd be canonized. There are still too many unexplored avenues."

The algorithm that hacked the VideoCrypt system is embarrassingly simple in construction. At the heart is a core function. This algorithm takes the message block of thirty two bytes and transforms it into an eight byte decryption key. Though the core function is simple, the fact that it is repeated 99 times makes the procedure of mapping an eight byte decryption key back to the original thirty two byte message packet extremely difficult.

This algorithm is more of a message digest than a true encryption system. It produces a digest of the thirty two byte packet. The packet contains the channel identification, time stamping and checksumming. In some respects this is an elegant solution to the problem of over the air addressing but in others it made the system totally vulnerable.

The result of using a single packet for authentication, addressing, checksumming and key generation, means that the system only has one layer of authentication. Hack that and the system is wide open. As a direct result of this, the options to recover from a hack are drastically reduced. Though apparently the Fiat Shamir Zero Knowledge Test may be implemented in the 8052, it does not appear to be in use. Otherwise things would have been different.

The fact that the decryption process can take place without a second layer of authentication points to a fundamental flaw in the design of VideoCrypt's access control. To put it simply: this hack should not have been possible with all of the claims that News Datacom made about their system.

The HLF algorithm transforms a thirty two byte message packet, m(0 to 31), into an eight byte decryption key, r(0 to 8). It is effectively a message digest. The core function, f, is non-linear in that it is difficult to reverse the function. If it was linear then it would be trivial to reverse. When there is an attempt to reverse the function, the result is not a unique result but rather a number of results.

The examination of the algorithm is in four stages. The first deals with the key selection and the compression of keys for use in limited memory microcontrollers such as the PIC16C54 and PIC16C84.

The second stage examines the core function. This is the function at the heart of the HLF algorithm. Essentially this is the main non-linear function in the algorithm. Trying to reverse the function produces a number of potential inputs that would provide the same result.

The third stage examines the algorithm in operation. The function is actually used ninety nine times. This makes the whole process exceedingly difficult to reverse.

The fourth stage examines the structure of the thirty two byte message packet, the various electronic countermeasures that Sky has implemented and the prospects for the security of the 09 smart card.

1: Key Tables And Structures

In the HLF algorithm, the keytable is 256 bytes long. This is rather large when considered for use in PIC processors. As the memory in these microcontrollers is limited, the keytable has to be compressed.

As it turns out, 256 is a very convenient number. It can be represented by two 16 byte arrays since 16 * 16 = 256.

So therefore by adding an entry from each array, it is possible to regenerate a complete 256 entry array. In this situation, addition is used. Multiplication or subtraction or any other function could possibly be used.

PIC Version of HLF 07 Key Table In Hexadecimal

65 E7 71 1A B4 88 D7 76
28 D0 4C 6E 86 8C C8 43
A9 EC 60 42 05 F2 3D 1C
6C BC AF C3 2B B5 DC 90
F9 05 EA 51 46 9D E2 60
70 52 67 26 61 49 42 09
50 99 90 A2 36 0E FD 39

In the PIC implementation of the HLF algorithm, the key table is only 56 bytes in length. This means that more than one 256 entry key table is stored in this 56 byte block.

Pic Version Of HLF Key Table In Decimal

101 231 113 026 180 136 215 118
040 208 076 110 134 140 200 067
169 236 096 066 005 242 061 028
108 188 175 195 043 181 220 144
249 005 234 081 070 157 226 096
112 082 103 038 097 073 066 009
080 153 144 162 054 014 253 057

Using the first thirty two bytes of the fifty six byte table, it is possible to generate the key values shown below.

In Hexadecimal Format:

Key_Col = {65,E7,71,1A,B4,88,D7,76,28,D0,4C,6E,86,8C,C8,43}

Key_Row = {A9,EC,60,42,05,F2,3D,1C,6C,BC,AF,C3,2B,B5,DC,90}

Column

65 E7 71 1A B4 88 D7 76 28 D0 4C 6E 86 8C C8 43
A9 0F 91 1B C3 5E 32 81 20 D1 7A F5 18 30 36 72 EC
EC 52 D4 5E 07 A1 75 C4 63 15 BD 39 5B 73 79 B5 30
60 C5 48 D1 7A 15 E8 38 D6 88 31 AC CE E6 EC 29 A3
42 A7 2A B3 5C F6 CA 1A B8 6A 13 8E B0 C8 CE 0B 85
05 6A EC 76 1F B9 8D DC 7B 2D D5 51 73 8B 91 CD 48
F2 58 DA 64 0D A7 7B CA 69 1B C3 3F 61 79 7F BB 36
3D A2 25 AE 57 F1 C5 15 B3 65 0E 89 AB C3 C9 06 80
1C 81 04 8D 36 D0 A4 F3 92 44 EC 68 8A A2 A8 E4 5F
6C D1 54 DD 86 21 F4 44 E2 94 3D B8 DA F2 F8 35 AF
BC 22 A4 2E D6 71 45 94 33 E4 8D 09 2B 43 49 85 FF
AF 15 97 21 C9 64 38 87 26 D7 80 FB 1E 36 3C 78 F2
C3 29 AB 35 DD 78 4C 9B 3A EB 94 10 32 4A 50 8C 07
2B 90 13 9C 45 DF B3 03 A1 53 FB 77 99 B1 B7 F3 6E
B5 1B 9D 27 CF 6A 3E 8D 2C DD 86 02 24 3C 42 7E F8
DC 42 C4 4E F6 91 65 B4 53 05 AD 29 4B 63 69 A5 20
90 F5 78 02 AA 45 19 68 07 B8 61 DC FE 17 1D 59 D3

In Decimal Format:

Key_Col = {

101,231,113,026,180,136,215,118,

040,208,076,110,134,140,200,067}

Key_Row = {

169,236,096,066,005,242,061,028,

108,188,175,195,043,181,220,144}

15, 145, 27, 195, 94, 50, 129, 32, 209, 122, 245, 24, 48, 54, 114, 236
82, 212, 94, 7, 161, 117, 196, 99, 21, 189, 57, 91, 115, 121, 181, 48
197, 72, 209, 122, 21, 232, 56, 214, 136, 49, 172, 206, 230, 236, 41, 163
167, 42, 179, 92, 246, 202, 26, 184, 106, 19, 142, 176, 200, 206, 11, 133
106, 236, 118, 31, 185, 141, 220, 123, 45, 213, 81, 115, 139, 145, 205, 72
88, 218, 100, 13, 167, 123, 202, 105, 27, 195, 63, 97, 121, 127, 187, 54
162, 37, 174, 87, 241, 197, 21, 179, 101, 14, 137, 171, 195, 201, 6, 128
129, 4, 141, 54, 208, 164, 243, 146, 68, 236, 104, 138, 162, 168, 228, 95
209, 84, 221, 134, 33, 244, 68, 226, 148, 61, 184, 218, 242, 248, 53, 175
34, 164, 46, 214, 113, 69, 148, 51, 228, 141, 9, 43, 67, 73, 133, 255
21, 151, 33, 201, 100, 56, 135, 38, 215, 128, 251, 30, 54, 60, 120, 242
41, 171, 53, 221, 120, 76, 155, 58, 235, 148, 16, 50, 74, 80, 140, 7
144, 19, 156, 69, 223, 179, 3, 161, 83, 251, 119, 153, 177, 183, 243, 110
27, 157, 39, 207, 106, 62, 141, 44, 221, 134, 2, 36, 60, 66, 126, 248
66, 196, 78, 246, 145, 101, 180, 83, 5, 173, 41, 75, 99, 105, 165, 32

The above matrix shows the results of adding the row values to the column values. Where the result is greater than 255, the entry is equal to the result minus 255. This will probably be more apparent in the decimal format example.

This 256 entry key table could be stored in a single array where microcontroller memory is not a problem. As a number of key tables are stored in the 56 byte block, a separate 256 byte key table would have to be stored for each entry. This is not a good method as a simple offset, as used in the algorithm would effectively create a new key table and a lot of hassle.

Addressing this matrix is straightforward. Since the Row and Column values are the values of in the two sixteen byte arrays, they can each be defined in terms of a nybble or half of a byte. The diagram below shows the matrix as addressed by this method.

Column (High Nybble)

Row (Low Nybble)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0F	91	1B	C3	5E	32	81	20	D1	7A	F5	18	30	36	72	EC
1	52	D4	5E	07	A1	75	C4	63	15	BD	39	5B	73	79	B5	30
2	C5	48	D1	7A	15	E8	38	D6	88	31	AC	CE	E6	EC	29	A3
3	A7	2A	B3	5C	F6	CA	1A	B8	6A	13	8E	B0	C8	CE	0B	85
4	6A	EC	76	1F	B9	8D	DC	7B	2D	D5	51	73	8B	91	CD	48
5	58	DA	64	0D	A7	7B	CA	69	1B	C3	3F	61	79	7F	BB	36
6	A2	25	AE	57	F1	C5	15	B3	65	0E	89	AB	C3	C9	06	80
7	81	04	8D	36	D0	A4	F3	92	44	EC	68	8A	A2	A8	E4	5F
8	D1	54	DD	86	21	F4	44	E2	94	3D	B8	DA	F2	F8	35	AF
9	22	A4	2E	D6	71	45	94	33	E4	8D	09	2B	43	49	85	FF
A	15	97	21	C9	64	38	87	26	D7	80	FB	1E	36	3C	78	F2
B	29	AB	35	DD	78	4C	9B	3A	EB	94	10	32	4A	50	8C	07
C	90	13	9C	45	DF	B3	03	A1	53	FB	77	99	B1	B7	F3	6E
D	1B	9D	27	CF	6A	3E	8D	2C	DD	86	02	24	3C	42	7E	F8
E	42	C4	4E	F6	91	65	B4	53	05	AD	29	4B	63	69	A5	20
F	F5	78	02	AA	45	19	68	07	B8	61	DC	FE	17	1D	59	D3

As was stated earlier, the 56 byte block can be used to generate a number of key tables. In the 07 it was used to generate three tables. In the example above, the first four rows were used to provide the two 16 byte arrays. By using an offset of 8 and an offset of 24, the arrays shown on the following pages are generated.

Offset = 8

Key_Col = {28,D0,4C,6E,86,8C,C8,43,A9,EC,60,42,05,F2,3D,1C}

Key_Row = {6C,BC,AF,C3,2B,B5,DC,90,F9,05,EA,51,46,9D,E2,60}

94 3D B8 DA F2 F8 35 AF 16 59 CC AE 71 5F A9 88
E4 8D 09 2B 43 49 85 FF 66 A9 1D FE C1 AF F9 D8
D7 80 FB 1E 36 3C 78 F2 59 9C 10 F1 B4 A2 EC CB
EB 94 10 32 4A 50 8C 07 6D B0 24 06 C8 B6 01 DF
53 FB 77 99 B1 B7 F3 6E D4 18 8B 6D 30 1E 68 47
DD 86 02 24 3C 42 7E F8 5F A2 16 F7 BA A8 F2 D1
05 AD 29 4B 63 69 A5 20 86 C9 3D 1F E1 CF 1A F8
B8 61 DC FE 17 1D 59 D3 3A 7D F0 D2 95 83 CD AC
22 CA 46 68 80 86 C2 3D A3 E6 5A 3C FE EC 37 16
2D D5 51 73 8B 91 CD 48 AE F1 65 47 0A F7 42 21
13 BB 37 59 71 77 B3 2E 94 D7 4B 2D EF DD 28 07
79 22 9D BF D7 DD 1A 94 FA 3E B1 93 56 44 8E 6D
6E 17 92 B4 CC D2 0F 89 EF 33 A6 88 4B 39 83 62
C5 6E E9 0C 24 2A 66 E0 47 8A FD DF A2 90 DA B9
0B B3 2F 51 69 6F AB 26 8C CF 43 25 E7 D5 20 FE
88 31 AC CE E6 EC 29 A3 0A 4D C0 A2 65 53 9D 7C

Offset = 24

Key_Col = {6C,BC,AF,C3,2B,B5,DC,90,F9,05,EA,51,46,9D,E2,60}

Key_Row = {70,52,67,26,61,49,42,09,50,99,90,A2,36,0E,FD,39}

DC 2D 20 34 9B 26 4D 01 6A 75 5B C1 B6 0E 53 D0
BE 0F 02 16 7D 08 2F E2 4C 57 3D A3 98 EF 35 B2
D3 24 17 2B 92 1D 44 F7 61 6C 52 B8 AD 05 4A C7
92 E2 D5 E9 51 DB 03 B6 20 2B 11 77 6C C3 09 86
CD 1E 11 25 8C 17 3E F1 5B 66 4C B2 A7 FE 44 C1
B5 06 F8 0D 74 FE 26 D9 43 4E 34 9A 8F E6 2C A9
AE FE F1 06 6D F7 1F D2 3C 47 2D 93 88 DF 25 A2
75 C5 B8 CC 34 BE E5 99 03 0E F3 5A 4F A6 EB 69
BC 0D FF 14 7B 06 2D E0 4A 55 3B A1 96 ED 33 B0
06 56 49 5D C4 4F 76 2A 93 9E 84 EA DF 37 7C F9
FC 4D 40 54 BB 46 6D 21 8A 95 7B E1 D6 2E 73 F0
0F 5F 52 66 CD 58 7F 33 9C A7 8D F3 E8 40 85 03
A2 F2 E5 F9 61 EB 13 C6 30 3B 21 87 7C D3 19 96
7A CA BD D1 39 C3 EA 9E 08 13 F8 5F 54 AB F0 6E

6A BA AD C1 29 B3 DA 8E F7 03 E8 4F 44 9B E0 5E
A5 F5 E8 FC 64 EE 16 C9 33 3E 24 8A 7F D6 1C 99

By using three offsets of 0, 8 and 24 respectively, the 56 byte table can be used to generate the three key tables shown. In their full expanded format, these tables would occupy 768 bytes. Some claimed that the 07 card contained the algorithms for the 06, 07 and 08 issue. If this is correct then the only apparent difference between the three issues is the code table. It also would seem that the three code tables would apply to each of the card issues. If this is correct then the system implementation would have been poorer than expected.

It would appear that the method of addressing the key tables is similar to that used in the S-Box routines in the DES. However the S-Box routines are designed to be very tough. It is not known if the key tables are as tough or indeed as non-linear.

Of course the standard fixed offset is a very conventional method of key generation. The system could be made more secure by using a pseudo-random offset for each packet. This possibility is dealt with in stage four.

2: The Core Function, f

The HLF algorithm produces an eight byte output from a thirty two byte input. There are eight byte wide registers r[0..7]. At any one time the function is working with two registers.

The core function, f, operates in a byte wide manner. Each register is only eight bits wide and has no carry bit. This means that all of the operations are one byte wide. Operations like additions or multiplications will therefore be lossy.

When two eight bit numbers are added, the result may be a nine bit number. As this function works in eight bits, this ninth bit is lost. To even reverse a simple multiplication by two of an eight bit number produces two possible inputs that would give the same result.

In machine code, a multiplication by two simply involves shifting the bits in the eight bit register one bit towards the left so that a zero appears in the least significant bit.

Example Of The Shift Left Operation:

Binary	Hex	Decimal	
1101 1011	D B	219	Original Value
(1) 1011 0110	1 B 6	438	Shift Left By One Bit
1011 0110	B 6	182	(Ninth bit discarded)

In this example, it can be seen that two multiply by two is merely a question of shifting all of the bits one step to the left. Of course to divide by two, it is necessary to shift the bits one step to the right.

Since the ninth bit has been discarded, the divide by two will produce the following:

Example Of The Shift Right Operation

Binary	Hex	Decimal	
1011 0110	B 6	182	
0101 1011	5B	91	Shift Right By One Bit

The problem is that we are not sure if the correct original value was 219 or 91. Since the ninth bit is discarded, both values will produce a result of 182 when multiplied by two.

The same arguments of bit loss apply with the simple addition of two eight bit numbers even when one of the numbers is known. There are two possible starting numbers.

So by combining a sequence of multiplications and additions in a fixed length register, it is possible to create a function that, while not being impossible to reverse as a one way function is, leaves a lot of doubt over what the original starting value is. This is effectively how the core function in the VideoCrypt 07 hacker algorithm works. It has an elegant simplicity that belies its complexity.

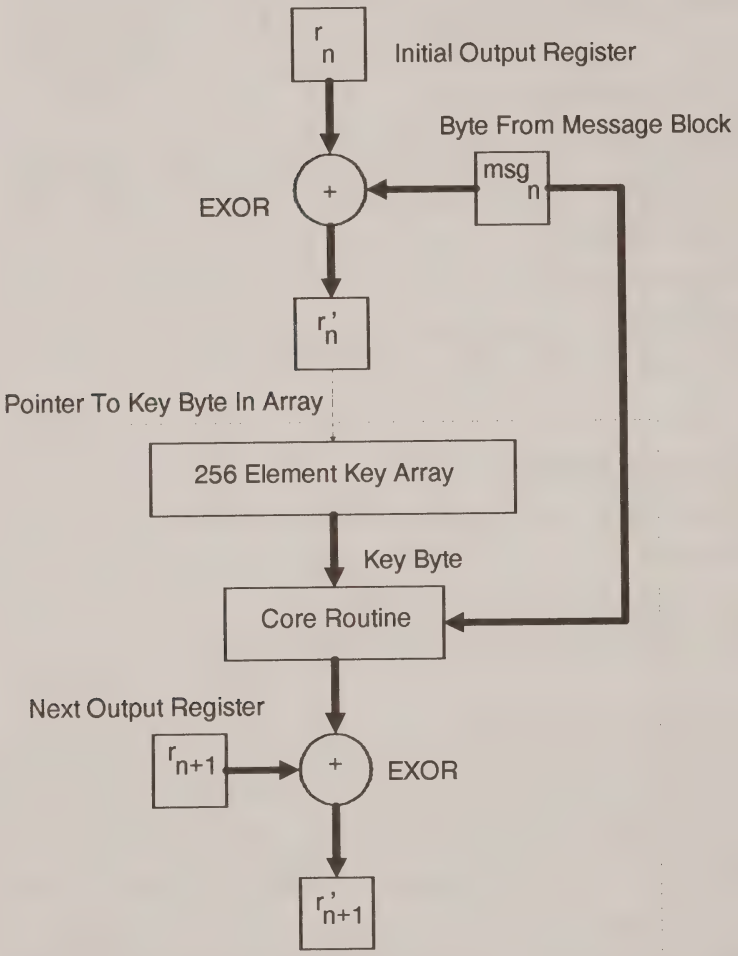
The fragment of C code below is the implementation of the core function. The input to the function, byte, is a byte from the message block.

```
/* Core Function */
void Owf(unsigned char byte)
{
unsigned char acc,kpoint,k1,k2;
/* Generate key */
r[Ppos]^=byte;
      kpoint=r[Ppos];
k1=key[Offset+(kpoint>4)];
k2=key[Offset+16+(kpoint&0x0f)];
acc=k1 + k2;
acc=~acc;
acc = (acc<1) | (acc>7);
/* Apply function to message byte, key and register*/
acc+=byte;
   acc = (acc<1) | (acc>7); /*shift left */
   acc = (acc>4) | (acc<4); /* swap nybbles */

Ppos++; /* increment Ppos */
Ppos&=7; /* this ensures that the value of Ppos is less
            than 8 /*
r[Ppos]^=acc;
}
```

r[Ppos] is the byte wide output register where Ppos is the pointer to the relevant register.

The first step in the function is to EXOR the message byte with the contents of the current output register r[Ppos]. This both changes the contents of the current output register r[Ppos] and creates a key pointer, kpoint.

The Ho Lee Fook Algorithm - Single Stage



In each case the width of each register is a single byte. The complete message block is 32 bytes wide and the complete output block is eight bytes wide.

The algorithm when viewed like this is surprisingly linear. The main thing to consider is that the function of adding or multiplying by two is lossy. Therefore to reverse one of these functions leaves two possible answers.

This key pointer, kpoint, is then used to select the bytes from the two 16 byte arrays. The bytes are selected by using the high nybble to address the first array and and the low nybble to address the second array. The procedure was detailed earlier. The offset referred to is effectively the value to select the correct table from the 56 bytes.

The two key bytes are then added. The result acc, is inverted and multiplied by two. This multiplication by two is the shift left routine.

This key is then added to the message byte. The result is multiplied by two. Then the high nybble is swapped with the low nybble.

The procedure to swap the nybbles is simple though in non programming terms it looks complex. Basically it is an extension of the shift right to divide and shift left to multiply concept. In order to divide by 16, we shift the bits to the right four times. The reason for this is that $2^4 = 16$. To multiply, it is a case of shifting the bits to the left four times. The OR operation is necessary to integrate the results of the division by sixteen and the multiplication by sixteen into a single number.

Example Of The Nybble Swap Operation:

Binary	Hex	Decimal	
1101 1011	D B	219	Original Value
0000 1101	0D	13	Shift to right four times
1011 0000	B 0	176	Shift to left four times
1011 1101	BD	189	Result of OR operation.

The next procedure is to increment the Ppos pointer so that it points to the next r[Ppos]. The value of Ppos is checked to see that it is only points to one of the eight output registers, r[0..7]. The contents of acc are then EXORed with the contents of the register r[Ppos].

The core function is relatively straightforward and could be implemented in a language other than C. The main problem is the definition of the byte wide registers. While this would not be a large problem in some of the more structured languages, it can cause problems in QBasic.

3: The HLF Algorithm In Operation

The strength of the HLF algorithm lies in the fact that the core function is applied ninety nine times. The thirty two byte message block is transformed into the eight byte output block. The application sequence is shown below.

Input Byte

msg[0...26]	Processed Through Function Once
0	Processed Through Function Twice
msg[27..29]	Processed Through Function Twice
msg[31]	Processed Through Function 64 Times

The thirty second byte, Byte 31, is intended to make it exceedingly difficult to reverse the algorithm. This byte is often referred to as the "destructor byte". The thirty first byte, Byte 30, is not processed through the core function. This byte along with bytes 27,28,29, is used to provide the checksum for the packet.

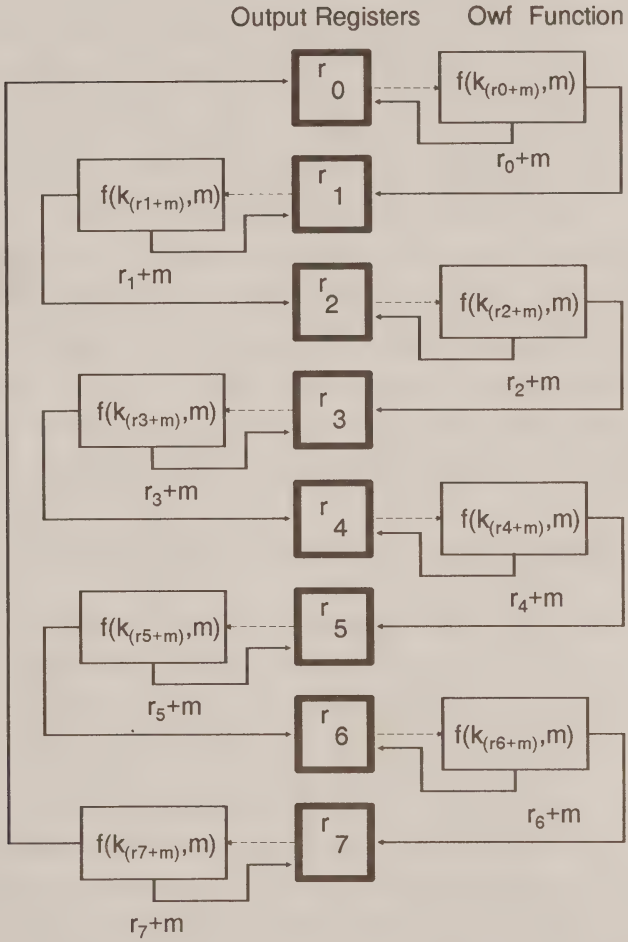
In the manner that the algorithm transforms the thirty two byte message block to the eight byte output block, it is more akin to a message digest. Instead of a single decryption key being extracted from the datastream, as is the case with VideoCipher and EuroCrypt, the whole packet effectively becomes the encrypted key.

If any of the bytes are wrong then the resultant output block will be wrong. In this respect it is very elegant. The integrity of the authorisation data, channel identification and decryption information is guaranteed. The official card will reject any packet that fails the checksum. This means that the card cannot be authorised by hackers who do not know what the card identity and checksumming routines are.

From the knowledge gleaned from the previous sections, it is now possible to draw a rather simplified model of the HLF algorithm in operation. The model shown is effectively cyclic.

The distribution of the bytes from the message block among the output registers is linear as far as byte 26. For the checksum, routine the pattern changes but after this routine, the pattern resumes the cyclic structure.

A Simplified Model Of the HLF Algorithm



The + in each case represents Modulo 2 addition or EXORing. The text r_n+m indicates that the message byte is EXORed with the contents of the register. Some of the EXOR stages such as the EXORing of the message byte, m, with the relevant output register, r, and the EXORing of the output of the function $f(k_{(r+m)},m)$ with the relevant output register, r, are omitted for clarity. To see how the individual stages are constructed refer to the diagram on page 6-40.

Distribution Of Message Block Bytes

Output	Message Byte											
0	00	08	16	24	--	31	31	31	31	31	31	31
1	01	09	17	25	28	31	31	31	31	31	31	31
2	02	10	18	26	28	31	31	31	31	31	31	31
3	03	11	19	*0	--	31	31	31	31	31	31	31
4	04	12	20	*0	29	31	31	31	31	31	31	31
5	05	13	21	--	29	31	31	31	31	31	31	31
6	06	14	22	27	--	31	31	31	31	31	31	31
7	07	15	23	27	31	31	31	31	31	31	31	31

*0 is where the value 0 is used instead of a byte from the message block. This happens for the first two rounds of the checksum routine. Where the symbol -- appears, the register is skipped. Also if you count the number of times that byte 31 is applied to each register, you will see that it is applied eight times to each register.

This pattern also repeats, though offset by one register, in the application of the output of the core function. The difference here is that the processing of the *0 bytes does produce different results.

Distribution Of Core Function Output Bytes

Output	Round												
0	--	07	15	23	30	35	42	51	59	67	75	83	91
1	00	08	16	24	--	36	44	52	60	68	76	84	92
2	01	19	17	25	31	37	45	53	61	69	77	85	93
3	02	10	18	26	32	38	46	54	62	70	78	86	94
4	03	11	19	27	--	39	47	55	63	71	79	87	95
5	04	12	20	28	33	40	48	56	64	72	80	88	96
6	05	13	21	--	34	41	49	57	65	73	81	89	97
7	06	14	22	29	--	42	50	58	66	74	82	90	98

The basic model shows that in each round there are changes to two of the output registers. The register at the start of the round has the message byte EXORed with it. This now becomes the key pointer for the core function. The output of the core function is then EXORed with the contents of the next output register.

The program shown below is the implementation of the HLF algorithm without the major checks for ECMs. Changing the message block is simply a matter of overwriting the current values and recompiling. It was written and compiled with Turbo C++.

```
#include <stdio.h>
/* This a model of the Ho Lee Fook Algorithm
as used in the hack on VideoCrypt. */
unsigned char key[56] = {
0x65, 0xe7, 0x71, 0x1a, 0xb4, 0x88, 0xd7, 0x76,
0x28, 0xd0, 0x4c, 0x6e, 0x86, 0x8c, 0xc8, 0x43,
0xa9, 0xec, 0x60, 0x42, 0x05, 0xf2, 0x3d, 0x1c,
0x6c, 0xbc, 0xaf, 0xc3, 0x2b, 0xb5, 0xdc, 0x90,
0xf9, 0x05, 0xea, 0x51, 0x46, 0x9d, 0xe2, 0x60,
0x70, 0x52, 0x67, 0x26, 0x61, 0x49, 0x42, 0x09,
0x50, 0x99, 0x90, 0xa2, 0x36, 0x0e, 0xfd, 0x39
};
unsigned char r[8]; /* This is the key output */
unsigned char msg[32]= {
 0xf8,0x3f,0x6a,0x29,0x51,0x19,0x01,0x8a,
 0xa7,0xbc,0x50,0xeb,0xec,0xed,0xee,0xef,
 0xf0,0xf1,0xf2,0xf3,0xf4,0xf5,0xf6,0xf7,
 0xf8,0xf9,0xfa,0x8c,0x7a,0x20,0xff,0x41
  };
  /* This is the messagepacket */
int Ppos=0, Offset=0;
/* Core Function */
void Owf(unsigned char byte)
{
unsigned char acc,kpoint,k1,k2;
r[Ppos]^=byte;
kpoint=r[Ppos];
k1=key[Offset+(kpoint>4)];
```

```
k2=key[Offset+16+(kpoint&0x0f)];
acc=k1 + k2;
acc=~acc;
acc = (acc<1) | (acc>7);
 acc+=byte;
 acc = (acc<1) | (acc>7);
 acc = (acc>4) | (acc<4);
 Ppos++;
 Ppos&=7;
 r[Ppos]^=acc;
}
void main (void)
{
unsigned char a,b=0;
for(a=0;a<8;a++) r[a]=0; /* initialise key */
if(msg[1]<0x33) /* Calculate Offset */
Offset=0x00;
else if(msg[1]<0x3b)
Offset=0x08;
else
Offset=0x18;

printf("Offset (in hex) = ");
printf("%X ",Offset)
printf("\n");
for(a=0;a<27;a++)
Owf(msg[a]);
  /* Checksumming Routine */
```

```
printf("\n * Checksumming Routine * \n ";
printf("Conditions: valid checksum r[a] = msg[Ppos] \n");
printf("If this routine is omitted then the algorithm \n");
printf("will decrypt any msg packet without actually \n");
printf("checking to see if it is valid. \n \n");
for(a=27;a<31;a++)
{
Owf(b);
Owf(b);
b=msg[a];
 printf("%X ", msg[a]);
 printf("%X ", r[Ppos]);
if(msg[a]!=r[Ppos])
 {putchar(7); printf("Invalid Checksum Result \n");}
else printf("Valid Checksum Result \n")
Ppos++; Ppos&=0x07;
}
for(a=0;a<64;a++) Owf(msg[31]); /* Apply Destructor Byte */
printf(" \n Message Block: \n");
  for (a=0;a<16;a++)
   printf("%X ",msg[a]);
   printf("\n");
  for (a=16;a<32;a++)
   printf("%X ",msg[a]);
   printf("\n"); printf(\n");
printf("The decrypt key is: \n");
for(a=0;a<8;a++) printf("%x ", r[a]);
}
```

4: Packets And Possibilities

There are essentially two packets in the VideoCrypt protocol that are most important in the descrambling of the signal. These are the 74h and the 78h packets. The lower case 'h' indicates that the numbers are hexadecimal. The numbers themselves are the instruction class.

The 74h packet is the message packet that the decoder sends to the card. The information in this packet is used to generate the decryption key. The decryption key is sent back to the decoder in the 78h packet.

In some respects the integration of the access control data with the decryption control data is elegant. It does mean less data to be transmitted. With a low over the air data rate, VideoCrypt is a prime candidate for such techniques.

The VideoCrypt system has three modes of scrambling: Hard Scrambled, Free Scrambled and clear.

The breakdown on the 74h packet is as follows:

Byte 00: Decoder Flags

Byte 01: Card Age Byte - Used as pointer to code table

Byte 02:

to Authorisation Data / commands

Byte 05:

Byte 06: Channel Identifier

Byte 07:

to Authorisation Data (Card Id Numbers)

Byte 26:

Byte 27:

to Algorithm Checksum Bytes

Byte 30:

Byte 31: Packet Checksum Byte (Modulo 256)

Byte 00 in the message block is used to signal the type of packet to the card. This allows the message packet to be used for purposes other than generating a new decryption key. From observation, the second nybble has the value 8 when there is a new key to be generated. Using this information the official card does not generate a new key on receipt of a message packet unless specifically instructed to do so. This facility allowed Sky to implement a countermeasure based on this aspect.

In the high nybble of Byte 00, three values have been seen; C, E, F. The actual value of the high nybble is a sum. The C value identifies the packet as an instruction carrying packet. Apparently the two lower bits are added to the C value and indicate the scrambling mode to be used. This may point to the following flag structure for the scrambling modes.

1100 1000 C8 Clear

1101 1000 D8 (?)

1110 1000 E8 Hard Scrambled

1111 1000 F8 Hard Scrambled

The problem here lies with the Clear Scramble mode. For the others, the generation of the decryption key relies on the authorised smart card. In the Clear Scramble mode, there potentially is no smart card in the slot. This means that the key has to be generated from some other data.

This other data is probably a table in the chip that Sky and News Datacom refer to as the Verifier. Strangely there is a large 256 byte table of data in the 8052.

The significance of the use of both F and E as the high nybble value has not been established. One theory was that the F indicated a Pay Per View event. Since this would give a high nybble of 1111, it would be the highest logical scrambling mode.

The card age byte is used as the pointer to the key tables to be used in the algorithm to decrypt the packet. In the 07 card there were three sets of code tables. In the present Adult Channel hack, there are five key tables in use and the key table is 96 bytes as opposed to the standard 56 byte table used in the 07.

The channel identifier byte ties in with one of the claims made about VideoCrypt. It was claimed that it could support 255 channels. Apparently these channels would be tiered in groups of eight channels. The correlation is that the single byte has 256 states.

Each channel is represented by a single identifier byte. The channel identifiers are given below:

01 Sky Movies

01 The Adult Channel

02 The Movie Channel

02 JSTV

03 Sky Movies Gold

08 TV Asia

0C Sky One

8C Bravo

As can be seen from the table, some of the channels can share some identifiers. This gives rise to the concept of channel groups. It is a method of effectively multiplying the tiering capability of the system. Of course the key table data would be different with each channel in a group. If the message packet is put through the algorithm with the wrong key table then the algorithm checksum will fail. As a result the card will return a null decryption key (all zeros).

Some form of programme identifier would also be required. For general use, this would not be critical but it would it would be essential in PPV applications. According to some reports, this identifier is defined as a number between 1 and 399.

The addressing on the VideoCrypt system appears to be part of the actual message packet. According to some reports it can be operated in a geographical manner as well as on a purely channel orientated basis.

The significance of bytes 2 to 5 is not clear but it is believed that they have something to do with the card turn on and turn off process. These bytes may contain the instructions to the card's access control routines concerning the data in bytes 7 to 26.

In the older formats of the VideoCrypt system, the enable and disable instruction was sent in message Byte 3. A value of 00h in this byte meant that the card addresses following the channel identifier were to be switched off. A value of 20h in this byte meant that the card addresses following the channel identifier were to be enabled. Other values such as 90h and 91h meant that the subscriber was to call a number regarding the programme or his subscription.

This pattern can be seen in the data snatch from the Sky channels in New Zealand. The problem is that the UK version has changed from this format. It is not known if the motivation for the change was the Kentucky Fried Chip hack. This hack kept checking the data packets for the turn-off instruction and rejected such packets. Of course the more elegant version of the hack would have read the card identifier number from the Quickstart card, stored it in the 8752 RAM and then check each packet for the turn off instruction for that particular card.

When the VideoCrypt system was launched here in Europe, the publicity brochures made great play of the fact that the decoder had a chaining facility. In order to use his new card, the subscriber had to insert his old card, remove it and then insert the new card. Apparently this procedure ensured that cards could not be passed around and that a decoder would be imprinted with a particular card identity.

The theory was that the cards would only work in the subscriber's own decoder. This was a simplistic and somewhat shortsighted facility. It precluded the possibility that the subscriber had more than one decoder and also the possibility that the subscriber would change decoders.

The original design of the VideoCrypt decoder, the SVA1, had a 256 bit EEPROM on the 6805 (ZC404044). The theory was that this was where the card identity information was stored. In later versions this EEPROM was integrated into the 6805 (ZC404047).

Another aspect that has fallen into disuse is the idea of a parental lock out card. This card was known as a Key Card. Apparently this card could be used to lock out certain channels. The reason for the dropping of this aspect is unclear but one indication is that it might have been too costly to implement with a large subscriber base.

The data traffic on the UK version of VideoCrypt is naturally a lot heavier and as a result, there has to be more than one format of card enabling and disabling message. After all, there are a number of channel tiering options. On the Sky card, the subscriber can have the following options:

Sky Multichannels Only

Sky Sport Only

Sky Movies Only

The Movie Channel Only

Sky Movies & Sky Sports

The Movie Channel & Sky Sports

Sky Movies & The Movie Channel

Sky Movies & The Movie Channel & Sky Sports

Sky Movies & The Movie Channel & Sky Sports

There are only four real channels in this combination. The Sky Movies Gold is not a stand alone channel as it is provided as part of another channel's subscription.

This may indicate that the lower nybble of Byte 02 is the channel designation for the packet for the UK Sky packets. Of course this byte may also be some form of programme identifier or counter. It seems from the 74 type packets shown below that the Sky New Zealand package is still using the original format.

Sky Movies - New Zealand

```
F8 0E 2E 00 00 00 02 7F B6 7E A1 E9
F8 0E 2E 00 00 00 02
F8 0E 2E 00 00 00 02
F8 0E 2E 00 00 00 02
F8 0E 2E 00 00 00 02
```

Sky Sport - New Zealand

F8 0E E4 90 D1 61 01 88 63 18 82 FF FF
F8 0E E4 90 7A 26 01
F8 0E E4 90 3F 51 01
F8 0E E4 90 4A 7A 01
F8 0E E4 90 07 37 01

Sky News - New Zealand

F8 0E E4 20 00 00 01 55 94 E4 C3 1B
F8 0E E4 20 00 00 01
F8 0E E4 20 00 00 01
F8 0E E4 20 00 00 01
F8 0E E4 20 00 00 01

Sky One - UK

E8 43 12 3B C1 12 0C B8 86 18 B2 3A
E8 43 62 D4 F5 00 0C
E8 43 42 96 13 14 0C
E8 43 4A 26 F1 79 0C
E8 43 06 4C 41 0E 0C

Sky Movies - UK

E8 43 12 15 EB 2C 01 B8 86 43 16 CA
E8 43 46 F0 31 0E 01
E8 43 46 F0 66 01 01
E8 43 5E 1D AE 49 01
E8 43 5A D5 74 6C 01

The data in bytes 7 to 26 are card identification numbers. Due to the method used, the card identification numbers (5 bytes) are transmitted in blocks.

With the geographical addressing, all cards in a specified area can be temporarily disabled for a particular program or event. Therefore the first few digits of the card identification number could be considered the area code. The UK has postal codes that apparently can narrow a particular code to a street or area of a city and it appears that the 09 cards were distributed on a regional basis.

Of course it would be possible that each geographical area would have a range of card identity numbers assigned to it. This would allow the subscription management centre to temporarily black out different areas. The process would simply involved sending a disable instruction and the upper and lower limits. The card identities between these limits would then be disabled.

As the card identifier used in the over the air addressing is five bytes long then the bytes 7 to 26 would support four complete card identifiers. The problem here is that the kill or blacklist capability is particularly slow when compared to a system like EuroCrypt.

The compromise is to group the cards to be killed so that the main part of the identifier, (the first four bytes of the five byte card identifier), could be transmitted in bytes 7 to 10 and the low byte of each identifier would be carried in the bytes 11 to 26. This increases the blacklist rate to about sixteen cards per message packet. Where padding occurs, it seems that it is the last byte that is repeated. When the card identification number is requested by the decoder, the response is a six byte identification. The unused byte may well be the entitlement byte.

The algorithm's checksumming routine is perhaps the weakest part of the system. Since the result of some of the operations are equal to known values in the message packet, it is a possible point of attack. Of course to balance this out, the destructor byte tends to compensate for this weakness.

The destructor byte is also the packet checksum. It is the value needed to bring the sum of the previous 31 bytes up to a multiple of 256. In this respect it is always predictable.

If the card enabling procedure is understood, a more elegant hack is possible on VideoCrypt. It would be possible to upgrade a Sky Multichannels card into a card capable of decoding all of the Sky channels. This would ruin Sky's subscriber management system and

all of the statistics gathered on subscriptions would be invalid. In many respects it would be the nineties version of the Musketeer hack on VideoCipher.

During the lifetime of the Ho Lee Fook hack, the possibility of this type of authorisation system attack existed. It is not known if it was actually used in a commercial application. Perhaps this would be killing the golden goose. The more likely explanation is that the PIC offered more revenue and less risk.

The Electronic Countermeasures

Before a change of card was contemplated, Sky and News Datacom would logically have to exhaust all possibilities. This meant trying to modify the datastream. The theory was that the hacker cards would malfunction and the official Sky cards would stay working.

The theory, like all theories was bounded by reality. With each ECM, Sky risked hitting their own cards as well as the hacker cards. In the end it looked like a trade-off between a maximum kill and an acceptable level of casualties. The terminology may sound militaristic but it should be remembered that what was happening was a war. Sky were fighting to get the maximum lifetime from their cards. The cost of losing for Sky was that of another card issue. Given the odds, Sky had already lost. The new card issue was inevitable and everything that Sky tried was an attempt at staving off the new issue.

The Zombie Fix

Like many other things in life, it was the first one that had the greatest effect. The first ECM carried out by Sky was named the "Zombie Fix". The hacker cards and chips were half on and half off. They were not dead but they were definitely not working. Sky cards being used on unauthorised channels were also exhibiting the same effect.

The checksum routine in the HLF algorithm had not been implemented by the hackers. As a result, the hacker cards and chips would process any message packet without checking if it was a valid packet.

The solution was to implement the checksumming routine. There are effectively two routines in the system. The first and most obvious is that the sum of all the bytes in the message packet is a multiple of 256. The end or destructor byte is the value necessary to bring the sum of the previous bytes to the multiple of 256.

New Code Tables

In September of 1993, Sky were forced to change to a new code table. Unfortunately the hackers were waiting for them. The code table was already present on some of the hacker PIC chips and as such the ECM had a rather limited effect.

The main problem for Sky was that the code tables appeared to be known by the hackers. As a direct result, the ECMs have been viewed as attempts to stave off the reality of a card change. A card change and its attendant expenses was the last thing that Sky wanted. Of course the channels on the Sky Multichannels package were not as eager to stay on a hacked system.

A further code change occurred around January 1st, 1994. This table was apparently the last. It was also hacked quickly enough to make Sky and News Datacom look like pure amateurs.

Though the key table block used by Sky was 56 bytes, they only used three key tables. The story floated by some sources was that the offical 07 card contained the key tables for 06, 07 and 08. Another explanation for the third key table was that it was the Pay Per View key table.

Pay Per View was abandoned on the 07 card after some problems with some IRDs. This problem meant that there were two versions of the 07 card. One of them did not have the PPV routines.

The strange thing was that Sky never used more than three tables though there were actually more possible tables in the 56 bytes. The offsets used were 0, 8 and 24. Perhaps the real reson for this was that the pressure to issue a new card was just too much - the hackers already knew the tables.

The standard practice with VideoCrypt was that each card issue had the key tables of the previous issue as well as its own. This enabled the changeover period between cards.

The 0xA Fix

On April 27th 1994, Sky implemented a rather simple but effective ECM. Many of the low priced cards on the market were hit by this ECM. The reason for this widespread effect was that many of these cards were clones of the better engineered cards. Unfortunately the people producing the clones had not as great an understanding of the system as they should have had.

The channel identifier byte, Byte 06, on most of the Sky channels is currently 0x0? where ? is the channel number. The high nybble is always zero. For example Sky Movies is 0x01. The transmission sequence of the message packets up to that date is shown below:

One Valid Message Packet

One Invalid Message Packet (Zombie Fix)

This produced an evenly timed scrambled - clear picture on the screen. The new ECM added a third message packet. The new 74 message packet sequence became:

One Valid 74 Message Packet

One Invalid 74 Message Packet (0xA?)

One Invalid 74 Message Packet (Zombie Fix)

This had the effect of making the scrambled time twice as long as the clear picture time.

The solution was simple. The software in the PIC had to test this byte to see if the high nybble was non-zero. If it was non-zero then the packet was to be rejected as invalid and a null key was to be sent back to the decoder.

The same applied to the OMIGOD software which was modified within a few minutes. The update for the affected PIC chips was as quick.

```
if ((msg[6] & 0xf0)==0xa0)
{
{for(a=0;a<8;a++) r[a]=0;}
  printf("\n");
     for(a=0;a<8;a++) printf("%x ", r[a]); printf("\n");
```

```
printf(" The 0xA ECM was detected \n");
printf(" The correct response from the card is \n");
printf(" shown above. \n");
}
```

Dark Wednesday And Beyond

It was getting a bit like that scene in Monty Python's "Holy Grail". You know, the one where the knight claims he is able to fight even after multiple limb amputations and decapitation. For at least a year, the VideoCrypt system had been totally and utterly hacked and Sky and News Datacom had tried everything short of a new card issue to stop the hack.

On May 18th, 1994 the 09 card went into operation and the hacker cards stopped. In the annals of satellite piracy, the day is known as Dark Wednesday. All over Europe there was panic though some were handling it better than others. Some card dealers had disappeared fearing the worst from their customers.

At first, there were hopes that it was just another countermeasure. The packet structure seemed much the same. The main difference was that message byte 1, the card age byte, now pointed to a table outside the regular three tables. It was the 09 card.

Though there are all sorts of rumours on hacks, one thing is certain. The 09 codes will be hacked. It is only a matter of time as the chip from the card has been popped. There are some worries over an unusual structure on the chip. This may be extra tables or some form of Pay Per View timer.

When the original Ho Lee Fook hack occurred, the resources committed were not even a tenth as strong as those arrayed against the 09 card. The OMIGOD hack opened up the structure of the VideoCrypt system to mass analysis. This hack is being used as the starting point for the hack on the 09.

Something more devastating than any of the previous hacks lies ahead for the VideoCrypt system. One working title is "DDT". In this case the initials do not refer to the ecologically unfriendly pesticide. The letters stand for Delayed Data Transmission.

6: Cracking The Code

The scrambled VideoCrypt signal can be recorded. Perhaps a Super-VHS standard video recorder may have to be used for the best results but the scrambled signal can definitely be recorded. So can the decoder - card traffic. By logging the message packets and the responses from a valid card, it would be possible to decode the recorded scrambled signal as it is played back through the VideoCrypt decoder. Instead of the valid smart card, a computer using much the same technology as the OMIGOD hack would provide the correct decryption keys.

The keys for a complete film or programme are distributed via Internet or a bulletin board system (BBS). With Pay Per View, the full set of keys could be available a few minutes after the programme ended. Thus anyone who wanted to watch the program would just have to download the keys and replay the tape. In some respects it would mirror the current situation in the USA with VideoCipher. The inversion being that the European situation would use the keys after the event whereas the US situation uses the Keys before the event.

For News Datacom and Sky, the problem is that all of the data required to decode the picture is transmitted with the scrambled video signal. Therefore a complete log of the card - decoder traffic would, theoretically, have all the necessary data to decode a recording of the programme. It is a nightmare situation. Unless Sky and News Datacom can discover the identity of the particular card has been used for this process, their system is totally vulnerable. The same form of hack will conceivably work on the EuroCrypt system

When VideoCrypt was launched, it was supposed to be the ultimate scrambling system. To date it has been the ultimate in one thing only - disasters. From the Infinite Lives hack to the Kentucky Fried Chip to the Ho Lee Fook, the system has been repeatedly hacked. The hackers now know more about the system than most of the channels that use it. Every one of the microcontrollers in the VideoCrypt decoders has been popped. Their programs have been dumped and analysed.

Perhaps the main problem is that the security overlay was not developed in an electronically hostile environment. This was evident from the papers presented in the Irish High Court. The software development of the access control and subscription management appeared to have been carried out in the USA and Israel. The people who developed it appeared to be very good academics and fell into

that old trap. They designed it to withstand attacks from people with minds like theirs'. You almost get the feeling that the mind of a hacker is alien to them.

As a system, VideoCrypt is actually good. It does have possibilities but the fact that it was designed in the eighties weighs heavily against it. The Frozen Architecture was the ruling format for scrambling systems but the smart card was adding some flexibility. The security of the system now only depends on the smart card. If the smart card can be reverse engineered, there is little that can be done to maintain the system's integrity. From all reports, it looks like the 09 smart card will be hacked.

VideoCrypt would have been a lot more successful as a sporadically deployed system. It does not appear to have been designed as a generic scrambling system, or indeed to handle the present volume of subscribers. Blacklisting in a system should be extremely fast. The problem is that it has become the de-facto scrambling system for English language channels. This has given News Datacom and Sky a monopolistic stranglehold on the English language satellite television market.

It seems that at this point in time the only things the future holds for VideoCrypt are hacks and a slow extinction as the digital systems come on-line. The response of News Datacom and Sky to these hacks will probably be the same - they will waste money on legal action rather than developing a more secure smart card aspect. Meanwhile the pirates will cut their system to shreds.

As in times past, the warm waters of the Caribbean beckon the European pirates. This time the target is the American DBS venture, DirecTv.

News Datacom are supplying the security overlay for this system. The security overlay, known as VideoGuard, is the same as that use by VideoCrypt. According to reports, the only differences lie in the algorithm and some of the procedures. Then it would not be much fun otherwise.

The same claims are being made about the DirecTv system as were made about VideoCrypt. All the same old waffle about how great the people who designed the algorithms are, how the card can be replaced if there is a hack, the wonderful adoring publicity pieces in the

trade publications. Strangely none of the DirecTv publicity mentions anything about the hacking of VideoCrypt and the effect of fiscal reality on the "Detachable Secure Processor" theory.

The question now is whether News Datacom will get it right this time? Or will the situation develop along the same lines as the one in Europe? Somehow, the latter may well be the case.

The 09 Algorithm 18:05:94 - 27:06:94

The origins of the 09 hack are definitely in question at the moment. It is not precisely known if there was a leak in the News Datacom - BSkyB operation or the code in the 09 smart card was obtained by other means. It is, however, clear that the code released only lasted a short time before being turned off

There are many theories about this code. Some consider it to be the 08 issue code while others consider it to be a subset of the actual 09 code.

From examination, it does seem incomplete. However many of the ideas used in the 07 code have been carried over into the 09 release. The original design concepts are there, but they have been modified. The intent of these modifications appears to be to make the algorithm more secure.

The main problem here is that the 09 release is not the complete 09 code. There are still some as yet undisclosed routines and code tables. The fact that this hack could have been ECMmed so easily is evidence.

The Key Tables And Key Selection:

The size of the key table in the 09 code is 216 bytes as opposed to a typical 56 bytes in the 07 code. The concept of code table reuse is present in the 09. There may well be a few more 216 byte tebles in the actual 09 code.

The segment of the code table to be used for key generation in each round is selected using an offset derived from the message packet. There are three known selections. Two of the selections allow the use of a single 64 byte array in the key generation. The other selection uses the EXOR sum of two 64 byte arrays.

In the 07 code the key bytes were used in pairs. There were two 16 byte key arrays. The arrays have been increased to 64 bytes each in the 09 code. Though most of the options in the version released use a single 64 byte array, there is a provision for a combination of two arrays. This dual array option was used up to 26:06:94.

The key combination function, addition in the 07 code, has been changed to EXOR in the version of the 09 code under examination. Though the reason for the change is not known, it could have been intended to frustrate attempts to read out the key bytes.

The 09 Core Function

This is perhaps the greatest change in the overall structure of the algorithm. Whereas the 07 code only operated on a pair of the output registers during any round, the 09 code operates on all eight of the output registers.

The fact that the contents of all of the eight change after each round means that the simplified attacks on the bytes before the checksum bytes in version 07 will not work with this algorithm.

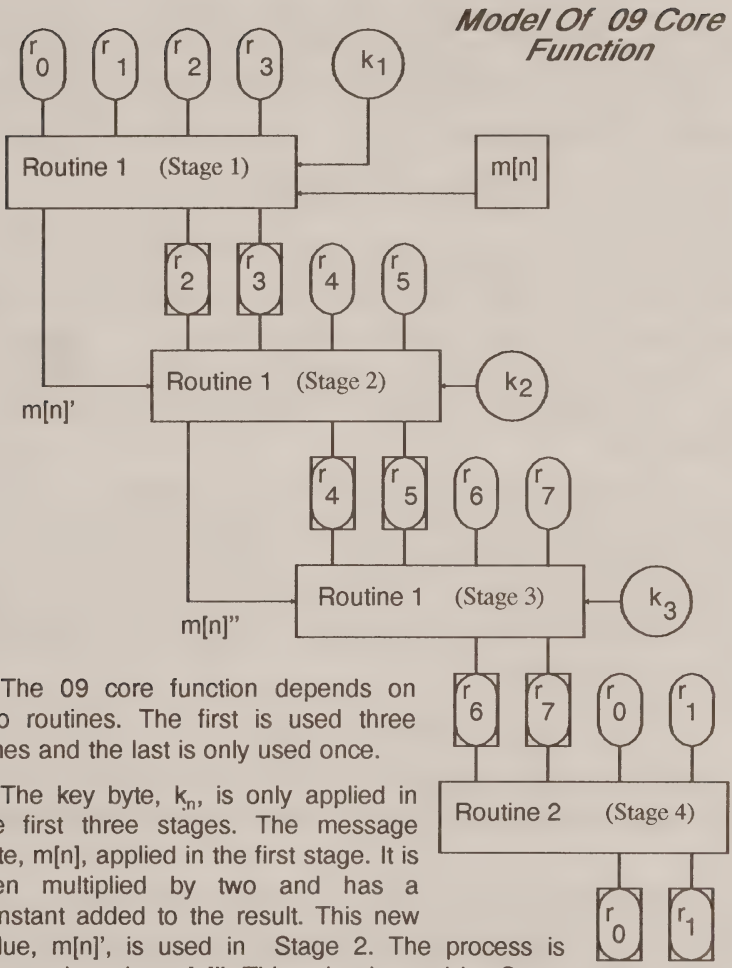
The structure of the 09 core function is effectively four routines. The first three are identical and operate on r[2 to 7]. The final routine, while being similar to the preceding routine introduces a number of constants. This routine operates on r[0] and r[1].

The first three stages use different keys. The pointer to the key byte is derived by ANDing the starting output register with 3Fh. This ensures that there are only 64 possible values for the pointer. This pointer value has an offset added to select the correct byte. This offset can be set using a byte in the message packet. In the version that Sky nuked, the following selection was used:

```
k1= r[i] & 0x3F;

k= key[k1] ^ key[k1 + 0x98];
```

The process used in both routines is multiplication. The result of the multiplication is a sixteen bit number. This result is broken into two bytes which are then combined with the contents the two output registers affected by the stage.

In the first routine, the multiplication operates on the combination of the message byte, the key byte and three of the output registers. The message byte is modified for stages two and three.



The 09 core function depends on two routines. The first is used three times and the last is only used once.

The key byte, k_n, is only applied in the first three stages. The message byte, m[n], applied in the first stage. It is then multiplied by two and has a constant added to the result. This new value, m[n]', is used in Stage 2. The process is repeated to give m[n]". This value is used in Stage 3.

Stage 4 uses a different routine to the previous stages. This particular routine is simlar to the previous one but it does introduce a number of constants. The key byte and message bytes are not used in this stage.

In each stage, the contents of only two registers are changed. In the diagram these are the boxed r_n registers. The rounded boxes are registers used in each round but the contents of which do not actually change.

The second routine multiplies the contents of output registers r[6] and r[7]. The high and low byte are distributed over r[1] and r[0]. The contents of these registers then have a constant added and also can be incremented by one depending on whether the result meets the condition of an IF statement.

The Structure Of The Code

The surprising thing about this 09 code is that uses the same 27 - 4 - 1 structure as the 07 code. The first 27 bytes are processed once each, the next four bytes are used to provide the checksum for the packet and the last byte is processed sixty four times.

The checksum routine is largely the same as that for the 07 except that it now checks the contents of output register r[7] against the message byte.

The subscription management software is dependent on this structure of the message packet. So only minor modifications to the sequencing could be made. The main changes would be in the card addressing section. The old format of addressing, as used on the Adult channel, is too vulnerable. On the 07 implementation, the card kill instructions were probably encrypted or at least changed enough to not be glaringly obvious.

After The ECM

The ECM effectively knocked out this code. However the change to the algorithm only appears to have affected the processing of the last byte.

Various options have been tried. The number of times that the byte is processed has been varied. The core function has been modified. The key tables have been alternated. None of these options seem to have worked yet.

At the time of writing there are reports that the full 09 code is on sale for three hundred thousand pounds. Of course this may well be a rumour or it could be, as many pirates believe, a sting orchestrated to destroy the market.

EuroCrypt Cracked

At the 1992 Subscription Television Conference in London, I called the EuroCrypt-M D2-MAC system "crap". I actually used that word because it looked like some very stupid mistakes had been made in its implementation. The system was utterly vulnerable to the McCormac Hack and according to all indications, the system was about to be seriously compromised.

It was a hot Friday afternoon in the middle of the wet English Summer. The conference was one of those overpriced self-congratulatory events that pad the corporate calendar. Most of the audience were asleep or braindead. It was hard to tell from the stage. Even the ensuing debate between Jean Pierre Coustel, the head of the France Telecom Visopasse program, and myself failed to wake some audience members.

Later that year, EuroCrypt-M was hacked. The results have been disastrous both for France Telecom and the channels using EuroCrypt-M. At the time of writing most of the channels using the system are still hacked. France Telecom has been spurred into legal action in Germany against Megasat, one of the main producers of hacker D2-MAC EuroCrypt-M cards.

This court action in Germany makes Sky and News Datacom look downright clever by comparison. Unfortunately the judge appeared to be classically educated and swallowed the France Telecom story about a secret key in the card being a trade secret. He allowed a temporary injunction against Megasat which stopped them selling hacker EuroCrypt cards.

In EuroCrypt, the critical element is the key rather than the algorithm. From most indications, the algorithm used was a modified form of the Data Encryption Standard. This indication was reinforced by a comment made at the 1992 Subscription Television Conference that EuroCrypt used the same algorithms as the banks. The banks use RSA and DES.

Of the two algorithms, DES was the more likely. The EuroCrypt-M smart card does not have the computing power to safely handle RSA as part of the control word generation. Therefore the algorithm used had to be DES or a variant.

The problem with DES is that it is heavily geared towards a hardware implementation. It can be difficult to implement in software even in a microcontroller. The EuroCrypt smart card is modelled on the 6805 microcontroller and runs at 3.5 MHz. Any modifications to the published algorithms would have the desired aim of speeding up the decryption process without weakening the security.

The most obvious modification was the elimination of the Initial and inverse Initial Permutations, (IP and -IP). A public domain computer program, NET_DES.ARC, pointed out that these permutations appeared to slow down the process when it was implemented in software. It allowed an implementation in software without these permutations. Even with these permutations removed from the implementation, the DES is still a good algorithm for use in a scrambling system. The only proviso is that the key handling protocol must be good.

The choice of a 56 bit key in DES means that, according to theory, a brute force attack where every key was tried would take a long time. It was calculated that with a computer completing a DES operation every microsecond, it would take over 2000 years to find an individual key. Of course these calculations were made prior to massively parallel computing. If there is one thing agreed upon now it is that the 56 bit key is not big enough to offer good security.

The main rules for key handling in DES are that keys should be random and should never have any part predetermined. If a a number of keys are common to a few channels then the security is reduced.

It appears that there might well be a common key table for FilmNet and TV1000. In the EuroCrypt equivalent of the VideoCrypt message packet, a pointer indicates which key is to be used to decode the encrypted control word.

Given what is about to happen to the EuroCrypt system in terms of hacking, the whole modified DES usage has become a severe liability. The new hack on EuroCrypt uses each pirate smart card as part of a virtual key crunching network. With a few thousand parallel processors crunching through the key tables, the time to discover a channel's key would be greatly reduced.

Video Manipulative Systems

The title of the chapter is "Video Manipulative Systems". A VMS is a system that digitises and scrambles the video. The key word is digitise. A digital system theoretically offers more security but in practice the system can be hacked because of flaws in the other areas of the system.

Perhaps with the sole exception of the B-MAC system all of the video manipulative systems have remained commercially secure on the video scrambling. The video on the VideoCrypt was hacked in real time using a rather fast supercomputer. Of course this hack was impractical for the purposes of commercial piracy.

The weaknesses that resulted in hacks have been in either the architecture of the decoder or its access control system. Of course a major factor in the security was that the hackers refused to attack what arguably was the strongest point of each system. It was almost as if the thought mode of the system designers was frozen in the attrittion warfare style of World War One. The hackers meanwhile use a more fluid approach.

The main element in the rise of video manipulative systems has been the low cost of video Analogue to Digital Converters, ADCs, and video Digital to Analogue Converters, DACs. This has of course created problems for some of the older VMS such as B-MAC. It has become possible for a hacker to build an economically feasible pirate video only decoder. The weakness that allowed the hack to succeed was the actual standard transitions in the waveform.

Most of the VMS in use here in Europe rely on smart cards to enforce the access control. This whole idea is now seen in a very jaundiced light. The attitude that smart cards are the panacea for piracy has evapourated here in Europe. In the few years that they have been employed on systems, they have suffered a number of hacks.

Where the hacks occur, the companies providing the access control act with alarming detachment. Most of them are perhaps used to dealing with bankers. In banking, the admission that a system is hacked is tantamount to suicide. This attitude apparently infected

these access control companies. The result on the channels using their systems was devastating and in some cases legal action against these companies for incompetence was probably justified.

The main problem appeared to be that the access control system provider had a "Screw You" agreement with the channels. It was irrelevant whether the system security remained intact, they got their money either way.

In the United States, the VideoCipher people are acting like ostriches. They believe that the addition of a smart card to their VideoCipher Plus system will confer some element of unhackability. Yes, these are the same people who believed that VideoCipher was hackerproof.

The outlook for DirecTv, the American DBS venture is similarly unsettling. They are to use the same security overlay, VideoGuard, as the VideoCrypt system uses. An article in a March edition of the American publication, "Satellite Retailer" brought to mind Hemmingway's quotation about the most essential piece of equipment for a journalist. The article claimed that there had been "no reports of a pirated VideoCrypt since its entrance into the market in 1989". Yeah right! Now this statement was made roughly one year after the Ho Lee Fook hack on VideoCrypt had started operating. VideoCrypt had been utterly and totally hacked for a year in Europe. This major fact had been neatly ignored. The sole aim of the article was to make the DirecTv system and News Datacom look good.

The article was typical of the ignorant and inane claims made in Europe by News Datacom. It looked like they were trying to pull the same "minimal information" operation on the press in the USA. When VideoCrypt was launched in Europe the praise in the satellite press was worse than a Mexico city wind storm.

This hacking activity here in Europe will spread to the USA. Links have already been forged. Perhaps there may well be an American version of that most elegant of hacks - the OMIGOD. It would be a nice irony if it was distributed via the Delphi system in the USA. The contacts are being made and now doubt as DirecTv launches, attempts will be made to hack it. It remains to be seen if the DirecTv system will fare as badly as VideoCrypt.

VideoCrypt

The VideoCrypt system was a good low cost attempt at a secure scrambling system. It was based on the premise that the smart card provided hackers with a moving target rather than a sitting one. When the smart card was hacked, the theory was that it could be replaced.

This theory did not work very well. By April 1993 the smart card for the Sky channels was totally compromised. It was not until Dark Wednesday, May 18th 1994, that the Sky smart card had been properly replaced. Even now the days are numbered. The actual 09 smart card is being reverse engineered and it looks like there will be another genuine hack on the VideoCrypt system. At the time of writing there are a number of hacks on the 09 card. The problem is that nobody is sure how long these hacks will last for.

There has already been one major hack on the 09 smart card and it looks like that now that the core function is known there will be more. The actual full source code for the 09 smart card is rumoured to be on sale for three hundred thousand pounds.

It was readily apparent from the start of the Ho Lee Fook hack that the VideoCrypt smart card system had been totally compromised, News Datacom and Sky acted strangely. Their claims of a replacable smart card became just so much hot air. They lumbered from one crisis to another. Their electronic countermeasures were defeated with startling rapidity. It was apparent to everyone in the Blackbox industry that their system was totally hacked. Yet they persisted in their ivory tower views and tried to pursue pirates through the courts.

The legal action was the last straw - these people were not playing with a full deck. They could not protect their own system using technological means so they tried to use lawyers to fix it. It was like using a band-aid to fix a decapitation but with far messier effects.

At this point in time VideoCrypt looks very old. But then it was developed in the mid eighties. For that time period it was an elegant compromise in terms of engineering.

When the system was launched, some of the public relations people claimed that it was the most pirateproof system yet devised. This pirateproof attribute was a myth. A myth is an attempt to explain

The cover page of the VideoCrypt European Patent Application

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 428 252 A2**

(12) **EUROPEAN PATENT APPLICATION**

(21) Application number: 90310131.9

(51) Int. Cl.⁵: **H04N 7/167**

(22) Date of filing: 17.09.90

(30) Priority: 14.11.89 IL 92310

(43) Date of publication of application:
22.05.91 Bulletin 91/21

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB GR IT LI LU NL SE

(71) Applicant: NEWS DATA SECURITY PRODUCTS LTD
Morning Post Building, Tong Chong Street
Quarry Bay, Hong Kong(HK)

(72) Inventor: Cohen, Michael
4/4 Frankfurter Street
Jerusalem(IL)
Inventor: Hashkes, Jonathan
75 Uziel Street
Jerusalem(IL)

(74) Representative: JENSEN & SON
8 Fulwood Place High Holborn
London WC1V 6HG(GB)

(54) **A system for controlling access to broadcast transmissions.**

(57) A system for controlling access to broadcast transmissions including a transmitter having a transmission encoder for scrambling the broadcast, a multiplicity of subscriber receivers, each having an identical receiving decoder, containing no secret cryptographic keys, for descrambling the broadcast and a plurality of selectable and portable executing apparatus each being operatively associatable with a receiving decoder at a partially different given time and each executing generally identical operations to generate a seed for use by the associated receiving decoder to enable the receiving decoder to descramble the broadcast.

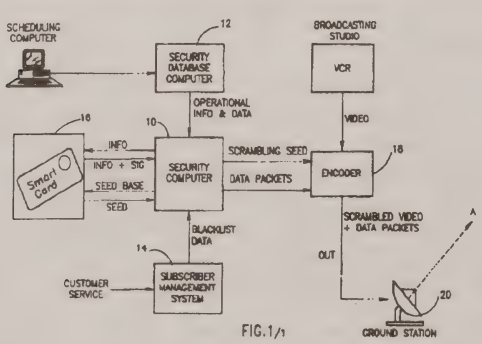


FIG.1/1

EP 0 428 252 A2

Xerox Copy Centre

a reality with the mental tools available. Therefore since the public relations people neither understood the abilities of hackers or the security of the system it would be, to them at least, pirateproof.

The philosophy of the VideoCrypt system is that of the Detachable Secure Processor. The decoder itself is merely a dumb terminal. The detachable secure processor is the smart card. Theoretically the smart card contains the critical data and the decoder contains nothing of significance. This "dumb terminal" idea has been echoed by and about News Datacom and Sky executives.

The decoder only contains the masked ROM 6805 and the masked ROM 8052. Both of these chips have been popped. Indeed the 8052 was unprotected. The 6805 contains most of the off-air data processing routines where as the 8052 is the housekeeper.

A great and respected mathematician, Professor Adi Shamir, was introduced as the creator of the algorithms used in the system. The News Datacom promotional material contained great claims of how the smart cards had to authenticate themselves every few seconds. As this authentication procedure was unbeatable, there was no way that a pirate smart card could be used with this system.

The Fiat-Shamir Zero Knowledge Test is the actual authentication procedure and it is indeed extremely difficult if not practically impossible to defeat when used properly. Right, I know what you are thinking - if the authentication procedure was so good then why was the system hacked with pirate smart cards? The answer to that will become glaringly apparent.

Apart from the obvious sources of information, there is another one. One that went by largely unnoticed. In 1990, News Datacom filed a patent application for a European patent on the VideoCrypt system. It did not specifically refer to VideoCrypt and as a result it went largely unnoticed. Instead most hackers went after the Thomson patents.

The application was filed by News Data Security Products Limited of Hong Kong. The inventors were Michael Cohen and Jonathan Hashkes of Israel.

A few years ago, Interspace published a rather irate letter from Jonathan Hashkes of News Datacom. In the letter he criticised all hacks on the system as being "Shillelagh Hacks". At the time I was not sure whether this was a personal insult or a demonstration of

ignorance. In a reply, I pointed out that a Shillelagh was a large stick for performing brain surgery without an anesthetic and the hacks on VideoCrypt would have a similar effect. Little more was heard of Mr Hashkes until the discovery of the patent application.

When I read the patent application, I could not help noticing that it cited the Baylin Publications book, "Satellite and Cable TV Scrambling and Descrambling" by Frank Baylin and Brent Gale. It was a particularly bad book on which to base judgments about the security of any scrambling system. Of course if they believed that that book was written by hackers then it is easy to see why VideoCrypt was hacked.

The summary of the invention, it was claimed that the invention, VideoCrypt, would provide improved apparatus and techniques for controlling access to broadcast transmissions. It would also include a public key proof, preferably a Fiat-Shamir public key proof, that would authenticate the smart card to the decoder.

The patent application gave very comprehensive information on the system architecture. Indeed it was startling to see how little the system had changed in implementation. It confirmed many of the theoretical outlines that had been built up from various sources over the last few years. There were even examples, in object code, of some of the programs used in the system.

The information in the patent application, while being old, does give an insight to the access control architecture in the VideoCrypt system. What emerges is more of a low budget system than contemporary systems such as EuroCrypt. More importantly for the era, the emphasis was on a cheap affordable solution rather than the all encompassing system.

The decoder is effectively a terminal and does not contain any keys. There is even talk of a mail box option for sending messages to individual users. In this respect it is similar to the old BSB EuroCypher system which had a rather elegant messaging system.

If anything, the VideoCrypt system drew heavily on previous systems though the use of the Fiat Shamir ZKT was new. Above all it seemed to be an attempt to get something in place that was effective, cheap and quick to assemble.

The VideoCrypt Subscriber Management System

The information on the VideoCrypt Subscriber Management System was largely gathered from the patent. Indeed it would seem that the main part of the structure of the SMS has not changed. The addressing is still carried out via the 32 byte 74h packets.

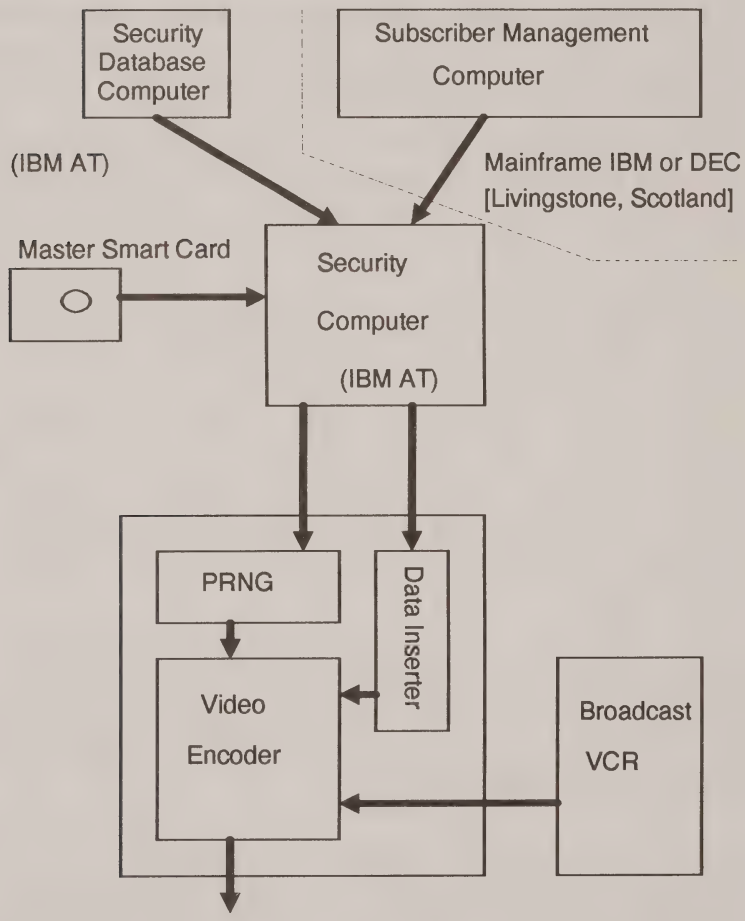
From the pictures in the News Datacom brochures, a large number of terminals are linked to the customer service computer. This would tend to indicate that it is perhaps a large network based on a mainframe. The actual brand of computer used as the service computer is not known but it given that most of the architecture is IBM, an IBM mainframe would not be unthinkable. In the early days Amstrad 1640s or Amstrad 1512s were in use as terminals though this seems to have changed judging from the pictures.

The subscription management system is, apparently, based in Livingstone in Scotland. They prepare a set of magnetic tape cartridges with customer details, such as subscriber numbers and channels purchased, which are then sent to News Datacom's premises in Maidenhead in England. The subscriber smart cards are personalised at the Maidenhead premises and are then shipped to the subscribers.

In the patent, the architecture of the subscriber management is based on individual computers. It would be more accurate to classify these elements in the structure as computer programs rather than distinct computers. They would of course be networked. Each channel would require its own separate master card or else the key could be generated from the 8052 verifier.

The generation of the key from the 8052 verifier would be the most logical method of generating the key for the free access mode. A large table of 256 bytes is present in each 8052. This could be used as the data for the public modulus for the Fiat Shamir ZKT, but it could also be used as the code table for the decryption key generation.

VideoCrypt Subscriber Management System



The subscriber management system is based in Livingstone in Scotland but the main studio facility is near London. This would imply that there is a leased line system (perhaps ISDN) between the points.

A master smart card is used to generate the seeds for scrambling though the verifier chip (8052) can also be used. This would probably account for the spurious reports of decoders decoding pay channels without cards.

The Security Computer:

According to the patent, this would be an IBM AT computer with multiple serial ports. The most likely configuration, today, would be a 486 or better with a multiple serial port card.

The function of the security computer is to act as a hub for the other computers in the network. It has to combine information from the Security Database Computer, the Subscriber Management System and the master smart card. The information from the Security Computer is passed to the broadcast VideoCrypt encoder.

In the patent, the implementation for one channel was shown. With the number of channels operating at the moment, a separate Security Computer would be required for each channel.

The Subscriber Management System:

This computer system is linked to the customer service computer and generates the list of cards to be turned off and the list to be turned on.

The patent mentions that the subscriber management computer system could be based on a mainframe. The logical option here would be an IBM mainframe as the rest of the system appears to be IBM flavoured.

The Security Database Computer:

The Security Database Computer supplies the Security Computer with the operational information on the programmes and pay per view. The operational information deals with items such as the identification, rating and duration and grouping of the programme being broadcast.

Video Scrambling

The scrambling technique used in VideoCrypt is line cut and rotate. The video is digitised and then cut at one of 256 possible points. The digitised video segments are then rotated about this point and the digital video is converted back to analogue.

The fact that the cut point is one of 256 points means that it can be defined as an eight bit word. This byte is supplied by a Pseudo Random Number Generator. The PRNG is sixty stages long and is reset approximately every two and a half seconds.

VideoCrypt transmits addressing and access control data in a few lines of the VBI. The data rate is slower than that of teletext. Each of the packets of data has a checksum. This checksum is a product of the active data in the packets.

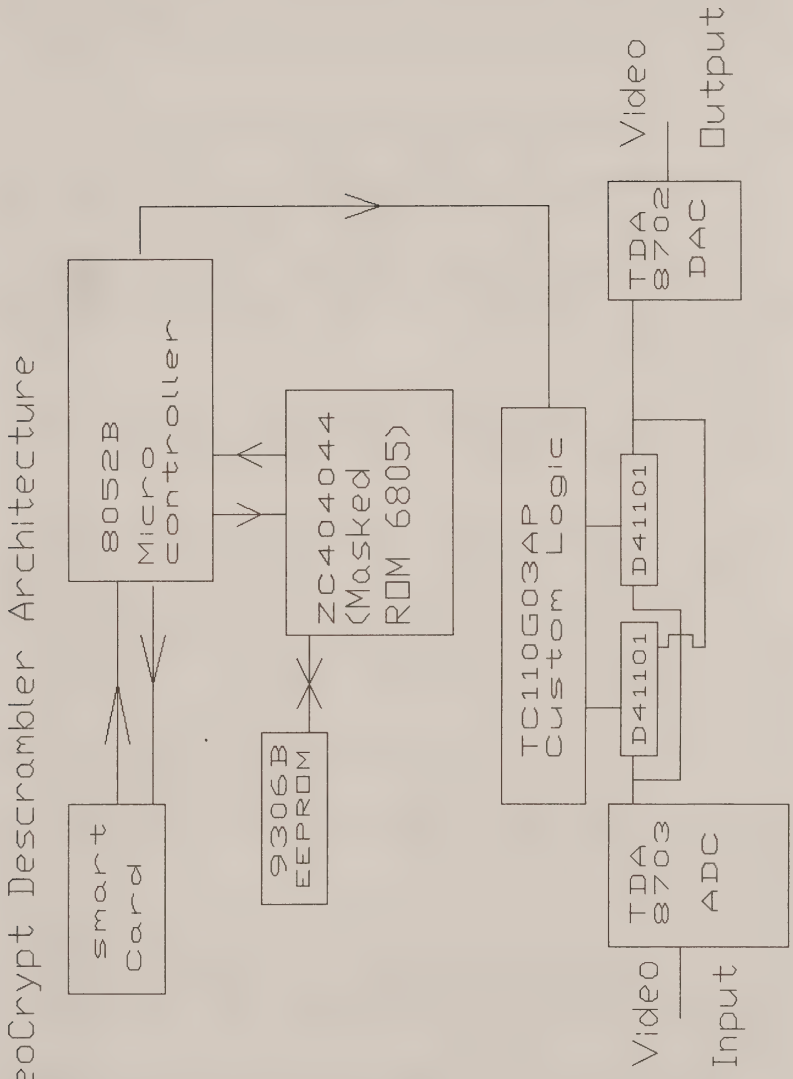
Only 585 lines or so in each frame are scrambled. This is to enable the VBI signals to be checked without descrambling the video. The reason for this is so that the signal quality can be checked on SMATV and cablenets without having to descramble the signal. It is a standard feature on most scrambling systems.

Decoder Architecture

The VideoCrypt stand alone decoder is a hybrid design. It uses both discrete components and surface mount components. This is necessary to reduce the size of the board. The board type used in the early stand alone decoders is SRBP or synthetic resin bonded paper. It is not the most reliable of board materials but it is one of the cheapest. It does reflect the television manufacturing industry as most of the boards in television receivers are SRBP.

In the IRD version, the power supply is part of the main receiver PSU. There are four voltage rails in the decoder: +21V, +12V5, +15V and +5V. The main part of the circuitry runs off of the +5V0 rail.

There are an estimated ten different VideoCrypt IRD designs on the market. Though the operation in each case is largely the same, they have been tweaked for operation with a particular receiver design.


VideoCrypt Descrambler Architecture
80528
Micro
controller
Smart
Card
93068
EEPROM
ZC404044
(Masked
ROM 6805)
TC110G03AP
Custom Logic
D41101
D41101
TDA
8703
ADC
TDA
8702
DAC
Video
Input
Video
Output

The circuit diagram for the VideoCrypt decoders are issued to authorised service centres on supposedly photocopy proof paper. This of course is a quaint if stupid move. Most television engineers have been able to obtain a circuit diagram as they have been on the market for the last few years.

The House Keeper Microcontroller:

The main processor in the descrambler is the 8052 from Intel. This is a microcontroller and has an on-chip ROM and RAM. There are also two types of this microcontroller available; the BASIC ROM version and the Mask programmable version. The version used in the descrambler is the Mask version. This means that there is an 8K program running the decoder. The 8052 can be forced to disgorge the control program.

Many veteran hackers who examined the Sky decoder were suspicious of the ease with which the 8052 could be forced to disgorge the control program.

There are a few theories as to why the ROM in this chip was not protected. The most obvious one had to do with the rate at which the chip failed. As this chip handled the card interface, it would be the one that the hackers would start to play with. As a result it would be the one most frequently destroyed "accidentally". Rather than have a service centre stocked with replacement 8052s, an EPROM version could be blown and inserted in place of the original.

The other theory is based on stupidity. If you have designed an invincible system, protecting the ROM would be just icing on the cake. VideoCrypt was far from invincible. The ROM in the VideoCrypt II decoder is protected but that was to little avail. It was quickly popped and examined.

Of course the fact that the program in the 8052 could be read and examined meant that the whole card to secure processor interface could be monitored and where necessary the data could be modified. This fact led to the one of the most devastating hacks on VideoCrypt - The KENtucky Fried Chip.

The information in the VideoCrypt patent application was largely duplicated in the VideoCrypt-I 8052 right down to that 256 byte data table. There are minor differences between the implementations but they are, apparently, largely the same.

Other aspects of the system became clear. The decoder could use both smart cards and memory cards. When the decoder was using memory cards, it would use an internal algorithm to generate the seed. This meant that a decryption algorithm had to be present in the actual decoder.

There is an element of the 8052 that is not in current use on the Sky channels. The Fiat Shamir Zero Knowledge Test is an integral part of the security of VideoCrypt. It is the one thing that, the brochures claimed, would stop the pirate clone cards.

In fact if the Fiat Shamir Zero Knowledge Test had been in operation then the 07 piracy could not have taken place. All the pirate cards contained was the algorithm and code table to descramble the video.

The Adult Channel is currently using a very old version of the VideoCrypt system and it periodically triggers the Fiat Shamir Zero Knowledge Test but strangely the pirate card passes the test. This does tend to point to something being very wrong here.

Shortly after the smart card is reset, it sends its identity number to the decoder. All of the pirate smart cards that I tested returned a string of zeroes. Their identity number was 00 00 00 00 00 00. The decoder did not reject this identity number and indeed I do not think that any VideoCrypt decoder rejected it. The most obvious hack trap was ignored. The decoder did not even check to see if the decoder number was false. Of course the hackers would try to play false identity numbers but at the very least the decoder should have rejected such an obvious fake identity number.

The Fiat Shamir packets transmitted by the smart card on the Adult channel are each 64 bytes of zeroes. Since one of the numbers being used in the process is zero then it would seem that the response is indeed correct however to allow such an obvious fake response.

The Fiat Shamir Zero Knowledge Test is actually a very difficult thing to fake. Indeed properly implemented, it would have made VideoCrypt a very difficult system to hack. The fact that the decoder has to contain the routines to execute the test points to where the problem lies.

Fiat Shamir Zero Knowledge Test In Operation?

```
RESET: 3F FA 11 25 05 00 01 B0 02 3B 36 4D 59 02 81 80
DCDR 72: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
CARD 70: 00 00 00 00 00 00
CARD 7A: D8 53 45 41 53 4F 4E 37 20 56 31 43 33 20 20 20
          30 30 3A 34 38 20 20 20 20
CARD 7C: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
DCDR 74: E8 42 3A 20 4B 1E 01 FB 7E 86 78 AA AB AD AE B2
          B5 B9 BB BC 00 00 00 00 00 00 00 DD FF 9E 0C CE
CARD 78: D3 5B 02 60 B9 65 6B 0D
CARD 7A: 80 53 45 41 53 4F 4E 37 20 56 31 43 33 41 44 55
           4C 54 43 48 41 4E 4E 45 4C
CARD 7C: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
CARD 7E: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
         00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
         00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
         00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
DCDR 80: 01
CARD 82: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
CARD 70: 00 00 00 00 00 00
DCDR 74: E0 42 3A 20 55 74 01 FB 7E 86 78 E2 E3 E4 E5 E6
       E7 E9 EA 00 00 00 00 00 00 E9 DD 33 D2 58
```

The datasnatch above shows the decoder requesting the card to authenticate itself. The card is a pirate one (actually the DDT running on a PC). As can be seen the ZKT fails but the decoder does not shut down. The decoder continued to decode the picture. The card identity number returned by the pirate card was 00 00 00 00 00 00. The decoder should have at least recognised this evidently false identity number.

What happens if the hacker can watch the whole protocol taking place and can actually emulate the protocols? The 8052 was unprotected. Its program was dumped and In Circuit Emulators, (ICE), were used to experiment with the program in operation in real time.

The routines dealing with the Fiat Shamir ZKT could quickly be established. The results would, hypothetically, set a flag in the program. Now what happens if the hackers could rewrite the 8052 program replacing the ZKT with a sequence of loops that provided a similar delay? To put it simply it defeats the purpose of ZKT. Of course rewriting the 8052 is nothing new to hackers. The KENtucky Fried Chip and the very first versions of the Ho Lee Fook proved that.

It is difficult to believe that the people responsible for the overall design of the VideoCrypt system could have envisaged the forces massed against them. Perhaps they really believed that they had invented an unhackable system. Though the overall design of the VideoCrypt decoder is good, you tend to get the feeling that the people who designed the operating system and implemented the authentication scheme were most definitely not hackers.

Perhaps some of the problems that plagued the VideoCrypt-I design have been fixed in the VideoCrypt-II decoder. There were some interesting claims made on the improved security of the system. Again the 8052 and the 6805 chips in that decoder have been popped and the programs are currently undergoing analysis.

The Secure Processor:

The real processing heart of the Sky decoder is the ZC404044 or in later versions the ZC404047. The earlier decoders have an eight pin 9306 EEPROM. The later versions incorporate the EEPROM data on the ZC404047. The control program is held in masked ROM and as such is very difficult to read. However it was not impossible to read. In fact popping this chip was an essential part of the hack.

The first problem here was to identify the chip. The incriminating text on the chip proved that the ZC404044 was a Motorola microcontroller. ZC was a prefix generally used for customised versions. There was one other way of getting confirmation - phone Motorola, the manufacturers of the chip, and ask them about the IC. The ZC404047 designation was replaced by a rather generic Thomson number but the fact that the chip was tracked down helped. It was a mask ROM version of a 6805 microcontroller.

The function of the 6805 is to act mainly as the over the air data demodulator. This information is actually given in the patent application though the specific chip type is not mentioned. It also passes the relevant data packets to the 8052 housekeeper.

Again the patent application is very specific about the actual traffic and protocol. It even gives the waveforms associated with the procedures. The main data packet passed to the 8052 is the 32 byte 74h packet.

Much of the on screen messaging is controlled by the 6805. It is effectively the main processor of the decoder. It also generates a new seed for the PRNG in the custom logic chip at the start of each field. The eight byte decryption key is apparently combined with the frame counter to produce these seeds.

The Custom Logic

TC110G03AP is custom logic. It handles the control of the video descrambling circuitry. This is also the most likely area for the PRNG. On some of the later versions of VideoCrypt decoders this part is labeled TCE PTV-2. The TCE possibly standing for Thomson Consumer Electronics. This IC also handles the clock generation for the whole decoder. The IC's clock is derived from a 28 MHz crystal.

According the to the information given in the VideoCrypt brochures, the PRNG or Pseudo Random Sequencer was sixty stages long. This is a very convenient length. As the eight byte hash function output carries the reseeding value and a possibly four status flags which are apparently unused.

The exact nature of the PRNG is not known yet. The chip also includes the multiplexing control circuitry. This generates the control signals for the video storage lines and switching.

The Video Descrambler

The video section of the VideoCrypt decoder is elegantly simple. The scrambled video is digitised by a TDA8703 ADC. This turns the video into a sequence of 8 bit words. The digitised video is then fed to a set of two FIFO memories. FIFO stands for first in first out. These ICs are capable of storing 910 8 bit words each.

Each FIFO holds one segment of the line so that reassembling the video is merely a question of switching between the two FIFOs when clocking out the data. The descrambled digitised video, with the segments in the correct order, is fed to a TDA8702 DAC.

The multiplexing and latching is controlled by the custom logic IC. The analogue video is then fed to the output stage. This stage is a discrete transistor design. The video signal is clamped and the on screen graphics are added. The resulting signal is filtered before being routed to the SCART connector or back into the receiver.

The VideoCrypt Card Protocol

There is a finite number of packet types in the VideoCrypt system. After a lot of observation and experimentation, the function of each packet is almost completely known. Some areas such as the card addressing have changed over the different card issues.

When compared with a system like EuroCrypt-M, VideoCrypt is indeed a very sparse one. There are only ten recognised packet types in use. At this stage it is not known if the VideoCrypt II protocol has any additional packet types.

Instruction: 70h

Direction: Card to Decoder
Length: 6 Bytes
Contents: Card Identification Number

Each smart card has its own serial number. This serial number is six bytes long and is split into three areas: the card issue byte, the card identification number and the checksum.

The card issue is represented by a single byte. The high nybble always seems to be 2. This may indicate that the card type is smart rather than a simple memory card. The low nybble gives the issue number. The current issue is 9 and the last issue was 7. The next issue will be A.

The second area is the card identification area. This is a four byte number that contains the card identity. The last area is a checksum for the card identity.

Instruction: 72h

Direction: Decoder to Card
Length: 16 Bytes
Contents: Previous Card ID, PPV and Tiering Information

When a card is inserted into the decoder, the decoder will send a message to the card containing the four bytes of the card ID and other information. The other information probably has to do with the authorisation level of the card, the amount of PPV tokens remaining and whether the card is being chained.

The chaining process was designed so that each decoder would be imprinted with a card serial number and to allow the credits or tokens remaining in old cards to be transferred to the new subscriber cards. The system was designed when EPROM cards were the dominant form of smart cards. The chaining process does not appear to be used in Europe.

Instruction: 74h

Direction: Decoder to Card
Length: 32 Bytes
Contents: Message block (addressing & key data)

This is the workhorse of the VideoCrypt system. This message packet carries all of the card turn on and turn off codes. It is also used as the data for the hash function that generates the decryption key.

The data in this packet has a 27 - 4 - 1 structure. The first twenty seven bytes contain the decoder flags, the card addressing instructions, the channel identifier and the card addresses affected by this packet. The next four bytes are a hash function checksum. When the packet is processed by the hash function, part of the results in stages 28, 29, 30 and 31 should equal the bytes in these checksum bytes. The card will reject packets that do not have a valid checksum. The function of the checksum is to prevent a chosen plaintext attack on the hash function or a third party authorisation of a smart card.

The final byte is a packet checksum. The value of this byte is that required to bring the sum of the bytes in the packet to a multiple of 256.

Byte 0 in this packet carries the decoder flags. It effectively tells the decoder how the packet is to be handled. The high nybble identifies the type of scrambling in use. A value of Cxh indicates that the channel is not scrambled. A value of Exh or Fxh indicates that the channel is hard scrambled. The Dxh value may indicate a free access mode of scrambling. The value x8h as the low nybble indicates that the packet is to be used to generate a new decryption key. The value x0h indicates that the packet is an information packet and is not to be used to generate a new key.

Instruction: 76h

Direction: Decoder to Card
Length: 1 Byte
Contents: The Authorise button has been pressed

This packet instructs the card that the Authorise button on the decoder has been pressed. If the programme is a Pay Per View programme then the card will deduct the correct number of tokens from the PPV reservoir.

This instruction was used by hackers when the 07 hack was in operation. When the Authorise button was pressed, the pirate card would cycle through all of the fixes for known ECMs stored in the card.

Instruction: 78h

Direction: Card to Decoder
Length: 8 Bytes
Contents: The Decryption Key

This is the eight byte decryption key generated by the hash function in the smart card. This key is passed to the Pseudo Random Number Generator in the Custom Logic IC. Only 60 Bits of this result is used to seed the PRNG.

Instruction: 7Ah

Direction: Card to Decoder
Length: 25 Bytes
Contents: On Screen Message data

The data in this packet is the text to be displayed on the screen. The text is displayed on screen in two rows of twelve characters. Depending on the state of the bits in the first byte, the message can be suppressed or shown. Currently on some of the Sky channels, the message "THIS PROGRAMME IS BLOCKED" is present but not shown on the screen. This indicates that the present 09 version of VideoCrypt is already being set for PPV on Sky channels.

Instruction: 7Ch

Direction: Card to Decoder
Length: 16 Bytes
Contents: Card ID, PPV and Tiering information

This packet of information appears to be the card ID, PPV and Tiering information. The fact that this message packet always precedes the Fiat Shamir ZKT sequence could indicate that this information packet is used in the ZKT.

Instruction: 7Eh

Direction: Card To Decoder
Length: 64 Bytes
Contents: Fiat Shamir ZKT X Value

This packet of data contains the X response from the card. The response is the result of $X=R^2 \bmod N$ where R is an arbitrary number. Though it is not yet known this number R may be taken from the code table.

Instruction: 80h

Direction: Decoder to Card
Length: 1 Byte
Contents: The Q Flag for the Fiat Shamir ZKT

In the Fiat Shamir ZKT protocol used in the VideoCrypt system there are two possible values - 00h and 01h. This byte tells the card how to calculate the response for the Fiat Shamir Zero Knowledge Test.

Instruction: 82h

Direction: Card to Decoder
Length: 64 Bytes
Contents: The Card response for the Fiat Shamir ZKT

Again the nature of this response depends on whether the Q Byte was 00h or 01h. This flag tells the card to generate the response Y. If the Q Byte is 00h then this response would be Y= R. If the Q Byte is 01h then the response would be Y= (R*S) mod N. R is a number from a table in the smart card and S is the card serial number.

The card would be authenticated by the decoder if the following results are obtained:

$Y^2 = X \bmod N$ [if Q=00h]

$Y^2 = (X*V) \bmod N$ [if Q=01h]

The decoder would have received V prior to the authentication process. This number V is the card identity number and S is derived from S= sqrt(V) mod N

Other Instructions?

At the time of writing, a number of other instructions that the card recognises have been detected. Though these instructions do not appear in the 8052 routines, it is not known if they control functions to be used in the near future or or are card personalisation instructions.

The "future use" theory has some evidence to back it up. Apparently when the digital radio system, DMX launches soon, it will use the News Datacom system as the access control system on its

audio subcarriers. The deal apparently allows DMX to use the Sky audio subcarriers and also means that Sky will handle the subscriber management.

Of course the personalisation theory could be valid as well. The new keytables would have to be loaded into the card along with other details at News Datacom's card processing plant.

The Fiat Shamir ZKT In VideoCrypt

As was mentioned previously, the only European channel that is apparently still using the ZKT as part of their datastream is The Adult Channel. The procedure is listed below.

70: Card sends V (card identity number to decoder)

7C: Card sends identification and N ? to decoder

7E: Card sends 64 byte packet X to decoder

80: Decoder sends Q byte to card

82: Card sends Y response to the decoder

70: Card sends identity number to decoder

The sequence above would follow the model for the ZKT presented in chapter 6. However the public modulus N may actually be sent by the card to the decoder as a part of the 7C packet. Then the Q byte would dictate the type of Y response and the card would send that response in the 82h packet.

The problem here is that the exact structure of the 7Ch packet is not known. This packet may contain the public modulus N as well as part of the the card identity number.

The ZKT obviously does not work on the Adult Channel. If it did it then the decoder would reject the pirate cards. Instead the pirate cards just keep on working. The ZKT packet sequence has not been seen on issue 07 or indeed issue 09 VideoCrypt. Naturally it is very strange that the most difficult part of the VideoCrypt system is omitted. Then it is probable, given the hacker knowledge of all of the programs in the decoder's microcontrollers that it could be written out of the 8052.

The VideoCrypt Hacks

The following paragraphs briefly detail the various hacks on the VideoCrypt system. Each hack is dealt with at length later in the chapter.

VideoCrypt is not as secure a system as it was in the eighties. Much of this can be blamed on the fact that hacker technology has advanced whereas VideoCrypt remained largely frozen in silicon. Other factors have also played a major part.

The first commercial hack occurred in 1990. The Morley Research hack was named after the company who initially marketed the hack. Unfortunately, such actions within the boundaries of the UK are illegal. Morley Research were persuaded to desist

The second hack was more or less known about among hackers though it was never believed feasible. It was when the bizoids got hold of it that it became a problem for Sky. The market was flooded with cheap little voltage limiters that stopped the smart card memory from being programmed. The name of this hack was the Infinite Lives hack.

The third hack detailed is the KENtucky Fried Chip. This one was a departure from the hacks that preceded it. It marked the first time that the actual software in the VideoCrypt decoder had been used against the system.

The fourth hack, the McCormac Hack, is one to which VideoCrypt has no defence. This hack is based on one of the fundamental flaws of VideoCrypt and indeed other smart card based systems.

The fifth hack is known as the Ho Lee Fook hack. The name of this hack is a phonetic spelling of the response of various hackers when they were first told of the hack.

This was the most effective hack that occurred on the VideoCrypt system. It offered proof that News Datacom's authentication routines were invalid or, at least, not used. The hack was a genuine Pirate smart card. Of course some would have seen this as a clone card but it was not. It did not rely on the use of a fake or clone master identity.

The sixth hack is known as the OMIGOD hack. It is also referred to as the SEASON7 hack. This hack differed from all of the previous hacks in that it was free. The original concept behind it was that it was to restore Star Trek to the viewers in mainland Europe who lost it when Sky scrambled. This is a computer program that allows the IBM compatible to drive the decoder as a virtual smart card.

The seventh hack is known as the DDT hack. Basically this is an extension of the OMIGOD hack. The different aspect is that it allows Delayed Data Transfer or Transmission. It is possible to record a scrambled program and then download the key stream from a BBS or an FTP site. Then by using the OMIGOD interface, the keystream can be used to decode the scrambled programme off tape.

Another hack on the video scrambling has been achieved. It is possible to decode the video scrambling in real time given enough computer resources. This hack was carried out by Markus Kuhn in Germany on a 40 RISC computer. The problem for the application of this hack is that not everyone has the facilities of a half a million dollar computer to decode the video. However it was a most elegant hack.

The Morley Research Hack

The Morley Research Hack of 1990 had Sky very nervous. Someone had found a way to stop Sky from turning off the cards. The basic method used was the interception and redirection of the write routine. This was carried out with a circuit that was connected between the card and the card reader.

The code and the diagram are from the original hack. This has been confirmed by reliable sources. This is, apparently another version. Since the operation was being run from a UK address, Sky soon paid a visit. Since it is technically illegal in the UK to hack Sky.

The software produces another card identification number for the decoder. A few years ago this particular hack was successful but apparently Sky bought a few and were able to stop the hack.

The basis for the hack is that it tries to confuse the decoder into thinking that the card that it has inserted has a different identity number.

8748 Microcontroller Program

```
0000 04 09 00 04 09 00 00 04

0008 09 23 13 39 27 3A 04 10

0010 14 58 D3 AC 96 10 8A 02

0018 F8 D3 6F 96 10 14 58 D3

0020 81 C6 48 FF D3 83 C6 4A

0028 FF D3 85 C6 4C FF D3 87

0030 C6 4E FF D3 89 C6 50 FF

0038 D3 8B C6 52 FF D3 8D C6

0040 54 FF D3 8F C6 56 04 10

0048 04 E8 04 F1 24 1B 24 38

0050 24 3C 24 45 24 49 24 6B
```

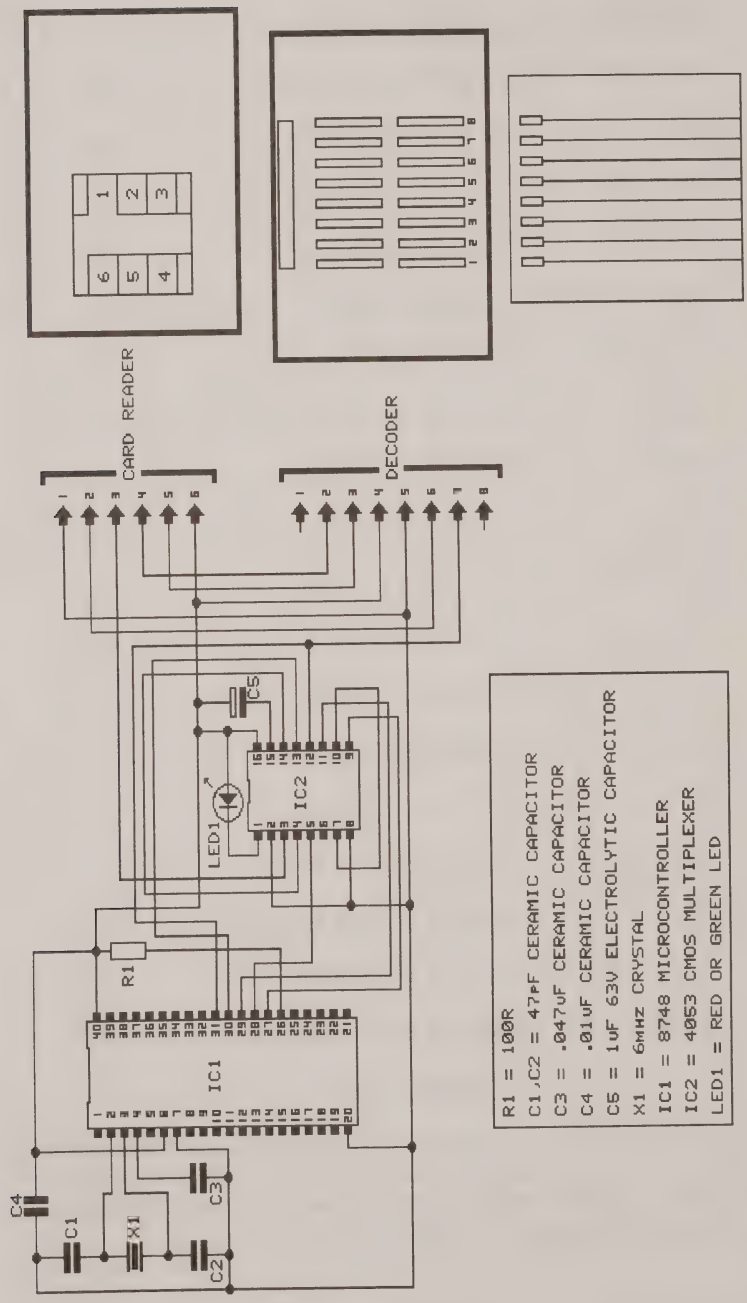
8748 Microcontroller Program (cont'd)

```
0058 09 47 67 F6 58 BE 06 EE

0060 5F BE 08 14 78 09 47 67

0068 FF F7 AF EE 63 14 78 14

0070 78 F9 A8 FA A9 FF AA 83

0078 BD 0D ED 7A 8A 01 9A 00

0080 83 AF 09 53 10 96 82 99

0088 10 34 89 BE 08 BC 00 FF

0090 F7 AF E6 95 1C 27 F7 F7

0098 43 10 39 34 92 EE 8F FC

00A0 53 01 D3 01 F7 43 10 39

00A8 34 92 23 13 39 34 92 34

00B0 92 83 AF 09 53 10 96 B3

00B8 23 15 39 34 89 BE 08 BC

00C0 00 FF F7 AF E6 C7 1C 27

00C8 F7 F7 F7 F7 43 15 39 34

00D0 92 EE C1 FC 53 01 D3 01

00D8 F7 F7 F7 43 15 39 34 92

00E0 23 13 39 34 92 34 92 83

00E8 8A 02 23 12 39 89 01 04

00F0 10 8A 04 BB 0A 14 58 D3

00F8 83 96 F5 23 FE 14 81 23

0100 FB 14 81 23 04 14 81 23
```

```
0108 07 14 81 23 0B 14 81 23

0110 FB 14 81 23 FF 14 81 EB

0118 13 04 10 8A 08 BB 18 14

0120 58 D3 E6 96 1F 23 85 14

0128 81 23 7F 14 81 00 00 00

0130 23 FF 14 81 EB 30 04 10

0138 8A 10 04 10 8A 20 23 12

0140 39 8A 01 04 10 8A 40 04

0148 10 8A 80 BB 0A 14 58 D3

0150 FC 96 4D 23 D5 14 B2 23

0158 4F 14 B2 23 E0 14 B2 23

0160 FB 14 B2 23 FF 14 B2 EB

0168 63 04 10 8A 80 14 58 D3

0170 8F 96 6D 23 B0 14 81 23

0178 15 14 81 23 06 14 81 23

0180 16 14 81 23 59 14 81 04

0188 10 9A 00 BD 07 ED 8D 8A

0190 80 83 9A 00 BD 09 ED 96

0198 8A 80 00 83 9A 01 ** **
```

Instructions:

Change bytes &174, &178, &17C, &180, &184 to random values from &00 to &FF to create a new card ID number. This will reduce the chance of the decoder receiving a deactivation code which matches that of the card the decoder thinks it has installed.


CARD READER
DECODER
IC1
IC2
LED1
R1
C1
C2
C3
C4
C5
X1
R1 = 100R
C1,C2 = 47pF CERAMIC CAPACITOR
C3 = .047uF CERAMIC CAPACITOR
C4 = .01uF CERAMIC CAPACITOR
C5 = 1uF 63V ELECTROLYTIC CAPACITOR
X1 = 6mHz CRYSTAL
IC1 = 8748 MICROCONTROLLER
IC2 = 4053 CMOS MULTIPLEXER
LED1 = RED OR GREEN LED

The Morley Research hack was intended to be constructed without a card reader assembly as found in the decoders. Instead an arrangement of connectors and a clamp were intended to hold the card in the correct position.

The unit was meant to be inserted between the card and the decoder. The connection to the decoder could be hardwired or a PCB with the card connector pad array could be used. The PCB card was the more difficult of the two. The actual fibreglass G10 PCB material thickness is about twice that of a normal smart card. The typical smart card thickness is 0.7 mm. The PCB had to be filed down with a commercial sander.

The actual circuitry of the Morley Research device can be constructed on a PCB or, with careful layout, Veroboard. The one thing that was decidedly unusual was the LED connected on the multiplexer. It would dump current into the multiplexer when turned on.

While the unit will not work on the present Sky cards, it did work well enough to provoke Sky. The modification Sky used apparently used a different address so the unit was left waiting for an instruction to write to a particular address that never arrived.

While this hack was defeated, it was the first attempt at interfering with the data flow between the card and the decoder. It proved to Sky that News Datacom and Thomson had not designed the most pirateproof system yet devised. Perhaps it was pirateproof to them because they could not figure out how to hack it. It was not the first time that somebody thought they had invented an unhackable system.

The hack might have been called the Yamamoto hack, for the situation was similar. During World War Two, the Japanese forces believed that they had invented an unbreakable cipher. They did not change it and transmitted all of their high security traffic in this cipher. Admiral Yamamoto was to travel by aircraft to one of the bases and his flightplan had been transmitted. A flight of American P-38 Lightnings was waiting for his aircraft.

The Infinite Lives Hack

The VideoCrypt decoder was supposed to be a dumb terminal devoid of any great secrets. Perhaps it was but there was a very serious flaw in the card. It required a voltage greater than 17 Volts to overwrite the card.

Rumours started floating around among the hackers that it was possible to modify the decoders so that the cards could not be invalidated. It was therefore possible for a Sky smart card to last indefinitely or at least until the next ROM change.

This hack was referred to as the "Infinite Lives Hack". Messages appeared on computer bulletin boards detailing the operation. An operation which involved snipping a few wires, soldering a few others and installing a zener diode.

Basically, the hack involved limiting the voltage on the card's programming connector. The voltage on this connector had to be in the region of 21 Volts for the card to be reprogrammed or written to. Cutting the voltage to this connector would have meant that the card and therefore the decoder would not work. Instead, the voltage was limited to a value, typically 15 Volts which would allow the card to operate but would not allow the card write operation to be successful.

A plethora of devices appeared on the market. The cost of these units ranged from about thirty pounds to over one hundred pounds. One pirate was offering a sample quantity of one hundred units for about four thousand dollars. Plainly these devices were little more that voltage limiters but they exploited a serious flaw in the VideoCrypt system. The publicity information on some of these products also claimed that they worked on D2-MAC Eurocrypt.

The Infinite Lives hack prevented the card's EPROM memory from being written to and therefore Sky could not turn off the cards. On the surface this would not seem too a serious problem. Of course when examined in detail, it was a problem of devastating proportions.

The actual problem lay with the Quickstart cards. A wonderful marketing invention by someone with a monumental ignorance of pay television security. These cards would be turned on by Sky over the air. They would allow a customer to walk into a shop, sign up and be authorised within a few hours.

There were so many dead people signed up for Sky that every day was a mini Last Judgment. False names and addresses were used with a professionalism that would impress the best Spies. Even some of the dealers got in on the act.

Of course most, if not all, of the Quickstart smart cards were destined for use in mainland Europe. The procedure up to the Infinite Lives hack was that the card would be authorised and then taken and kept out of a decoder for a month or two. Sky would send out the card identity in the blacklist at various times and since the card was not in a decoder it could not be switched off. The blacklist is transmitted on all Sky channels for maximum effectiveness.

The Infinite Lives hack caused a mushroom effect in the trade of the Quickstart cards in Europe. It was now possible to get a card that could not be switched off and was valid almost indefinitely. Normally if a Quickstart card in Europe gets nuked, the supplier has to provide another. The Infinite Lives hack meant that the risk of the cards being switched off was minimised. The cards held back in reserve by the suppliers were immediately brought on to the market.

The situation was getting out of hand and Sky were forced to act. They brought out a new card issue. The Version 06 cards incorporated a voltage tripler on the card wafer so that the Vpp voltage was not necessary. This solved the problem. It was not a cheap solution. It was estimated that it cost Sky over £7 million to replace the cards.

Sky's recovery from the Infinite Lives hack was a perfect demonstration of the main strength of smart cards. It allows the recovery of a compromised system. Smart cards are not impossible to reverse engineer, it is just expensive and hard to do so. The periodic change of cards is more of a deterrent to hacking than a card change when the system is compromised.

While the smart cards on the Sky services are issue 07 versions many of the other VideoCrypt services are using old issue cards that may well be susceptible to this hack. In many cases, it is not economically feasible for the channel to upgrade.

The amazing thing is that Sky and News Datacom had a very good opportunity to assess the scale of the Infinite Lives Hack and they never took it.

If they had included a routine in the 06 issue smart cards to test the EPROM write voltage, then it would have been possible to switch off the cards in a modified decoder. Of course the message "Please Contact Sky" could have been flashed up on the on screen graphics. The user of the hacked decoder would then have to telephone Sky to have the card turned on again. That way Sky could make a database of the hacked decoders.

There were some rumours at the 1992 Cable And Satellite Show that there was another modification to stop the cards getting turned off. It involved using a capacitor to skew the turn off data.

At the Subscription Television 1992 conference a delegate from News Datacom said that the fault for this hack lay with the card manufacturers rather than News Datacom. This was a rather strange statement considering that it would only require a few bytes of code to check whether the card had been written to. The same type of check could have been used to check if a KENtucky Fried Chip was in operation.

The crypto processor would have been instructed over the air to read a certain address in the card's memory and store the result as (A). Then it would have been instructed to write the new data, (B), to the address. The next step would be to read the new data from that address and store the result as (C).

The check is simply a series of comparisons.

1. **(A) should not equal (C)**

2. **(B) should equal (C)**

If either of these comparisons fail then the card cannot be written to and either the decoder has been modified for the Infinite Lives Hack or the KENtucky Fried Chip Hack

The KENtucky Fried Chip

The KENtucky Fried Chip may well be the greatest threat that Sky has faced so far. It is certainly the one hack that questioned the credibility of VideoCrypt as a viable scrambling system.

In one fell swoop it removed what is supposed to have been one of the strongest points of the VideoCrypt system - its over the air addressing.

The KENtucky Fried Chip worked by stopping the turn off codes being sent to the card. The card cannot be turned off. The card write routines have either been altered or completely removed. This by extension would mean that the card could not be authorised for other channels while the KENtucky Chip is in operation.

The name of the chip is a hacker's joke. It is named after the Sky's head of security Mr. Ken Crouch. Apparently he was being too successful in stamping out some Grey Market card operations.

VideoCipher II and EuroCypher used the philosophy of the Embedded Secure Processor. VideoCrypt relied on the Detachable Secure Processor philosophy and reduced the decoder to the status of a dumb terminal. There are some good arguments on each side.

To date it has been the Embedded Secure Processor systems that have suffered from piracy. VideoCipher II and FilmNet's Digital Audio have been hacked proving that the Embedded Secure Processor is anything but. EuroCypher was BSB's system. The amount of hackers trying to hack a system is a very good gauge of the success of a channel. BSB was considered by the Blackbox Industry to be a waste of time.

The fatal flaw in the VideoCrypt decoder was the unprotected 8052. This microcontroller handles the decoder housekeeping. It also handles the secure microcontroller - card interface.

It is standard procedure to blow the read fuses in decoder microcontrollers. This prevents unauthorised viewing of the stored program. Strangely, the read fuses on the official 8052 were not blown. In the Blackbox Industry this was looked upon as a screw-up of the highest magnitude. There may have been a valid explanation though.

Apart from the power supply section, the commonest failed component in the faulty VideoCrypt decoders is the 8052. In light of recent hacks, this problem would have increased. It would therefore make sense if it was possible to replace the chip without having to purchase an official model.

Many service centres will, in the case of a failed 8052 either replace it with an 8052 from a junked decoder or with an 8752 programmed with the program from an official 8052. Perhaps Thomson and News Datacom had this in mind when choosing not to blow the read fuses.

Sky and News Datacom successfully countered version 1.0 of the KFC. Version 1.1 was actually ready for launch when Sky issued the 07 smart cards. The software in the new batch was different from the previous batch. As a result, the version 1.0 and 1.1 KFCs did not work. Then there is always version 1.2.

News Datacom do not seem to have learned very much from the VideoCipher II fiasco. One of the first hacks used a piggy back arrangement for the EPROM. The hacker EPROM and the official EPROM were mounted on a PCB with a multiplexer and a DIL socket. Whenever necessary the official EPROM could be switched back into circuit.

The logical progression of this would be a KFC and the official 8052 on PCB with multiplexing. The multiplexing would be controlled by a fast third processor. The KFC and the official 8052 would be running in parallel. When the validity of the official 8052 is checked, the third processor can return the output of the official 8052. The third processor would have to interpret the commands to run the validity check.

The McCormac Hack

When the VideoCrypt system was launched, it was touted as the most pirateproof system yet devised. There were a few good reasons for their confidence. It used a SMART card. It used the security algorithms of Professor Adi Shamir of RSA fame. It took fifteen seconds to figure out the hack. Five to crack it and ten to write the hack down.

The McCormac Hack is a theory invented to check the security of a SMART card based system. It seriously upset the people who believed that SMART cards are totally pirateproof. Indeed the insecurity of the smart card based systems has been repeatedly demonstrated over the last few years.

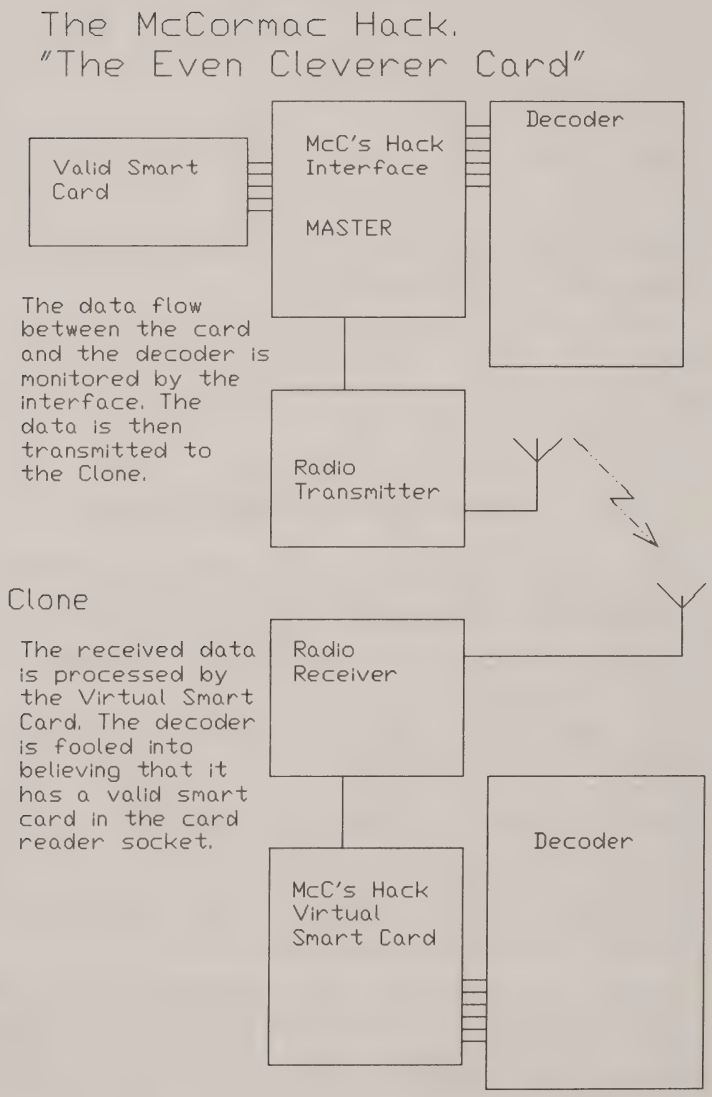
The theory is not restricted to SMART card systems. It can be applied to any system using more than one microprocessor in its architecture. This category incidentally includes most of the scrambling systems of the last few years

The McCormac Hack Theory

The most vulnerable area of any multi microprocessor based descrambler is the data flow between the microprocessors. If this data flow is accessible to hackers, then the system may be fatally flawed. If the data flow can be used to activate other descramblers then the system is, not to put too fine a point on it, dead.

The VideoCipher II system was hacked because data could be extracted from the descrambler and the data flow in the control architecture could be modified. One of the resultant counter-piracy operations involved encapsulating the descrambler's control section in epoxy resin. Of course reports reached Europe about these decoders overheating and cooking out. Very few if any manufacturers coat their decoder printed circuit boards in epoxy resin. Only some of the older cable descrambler designs have epoxied PCBs.

SMART card based systems are vulnerable because the data flow between the card and the descrambler can be monitored and used to operate another descrambler. It is not essential for the contents of the data flow to be understood by the hacker. In the case of a secure crypto system as used by VideoCrypt, it is likely that everybody including the designers understand the data.


The McCormac Hack.
"The Even Cleverer Card"
Valid Smart Card
McC's Hack Interface
MASTER
Decoder
The data flow between the card and the decoder is monitored by the interface. The data is then transmitted to the Clone.
Radio Transmitter
Clone
The received data is processed by the Virtual Smart Card. The decoder is fooled into believing that it has a valid smart card in the card reader socket.
Radio Receiver
McC's Hack Virtual Smart Card
Decoder

The data flow between a SMART card and the descrambler is serial data. Therefore the data is in a more vulnerable state than parallel data because it is easily transmittable. It has to be. Otherwise the link between the card and the descrambler would fail and the descrambler wouldn't work.

The McCormac Hack involves using this data flow between the processors to activate more than one descrambler with one card. Theoretically all descramblers in an area can be activated using this method.

The essential factor in this hack is the method used to convey the pirated data. Since the data is continually changing, options such as a key pad or EPROM are ruled out. This leaves telephone modem and radio transmission as the remaining candidates.

The telephone modem is a nice secure method. it is also a very costly method for a hacking operation. Perhaps where there are reasonable telephone charges this method of distribution would be feasible.

This leaves radio transmission as the only viable method of transmitting the pirated data. The fact that it may be illegal to transmit without a licence is of little consequence. This is a pirate operation we are talking about here!

The radio equipment required for this hack can be as simple as a modified radio control system for models or as complicated as an encrypted datastream system.

Naturally there are other factors involved in the hack. The use of a multi microprocessor system means that the equipment at the transmission end has to be complicated. The use of another descrambler's data stream will require the clone descrambler's circuitry to be synchronised with the master descrambler.

When the SMART card is inserted into a descrambler, the descrambler's processors are synchronously reset. This would have to occur when each clone descrambler is switched on to the scrambled signal. At the simplest level, some form of reset signal would have to be sent every few seconds. The receiving end would also require some circuitry that would only reset the microprocessors once and ignore all other reset pulses.

The best way of describing the hypothetical receiver is "An Even Clever Card". It would consist of four elements. The first would be a radio receiver. This would probably be a UHF type as the antenna size could be reduced. The second element would be the data decoder. The data would have to be protected from unauthorised piracy. The third element would be the microprocessor control circuit. The forth element would be the interface circuitry. This circuit would connect the Even Cleverer Card to the descrambler via the descrambler's card socket.

In some respects it could be argued that the Delayed Data Transfer hack is an extension of the theory. But it does take not take place in real time. The original theory was that the hack was to be a real time hack. However, the knowledge available now was definitely not available at the time of the original theory. Nobody back then thought that someone would be stupid enough to design a recordable scrambling system. It breaches one of the main rules of cryptology - give the opponent as little ciphertext material as possible to work with. Making the scrambled signal and control data so easily recordable clearly broke that rule.

It is of course very difficult to envisage a totally secure system. The more you hack, the more this point is apparent. Perhaps the only solution for any reasonable security is to use ASICs for the access control and the scrambling. Using conventional microcontrollers is a relatively cheap solution but it is also a fatal one. The more a hacker knows about a system, the closer that system is to being compromised.

The Delayed Data Transfer hack would not have been possible if VideoCrypt was not thoroughly examined before hand. The use of conventional microcontrollers had a lot to do with this understanding. The Blackbox industry in Europe had been frequently popping similar microcontrollers when copying FilmNet Satpac decoders.

Perhaps the next test of the theory will be the DirecTv system in the USA. It will be interesting to see if any of the lessons News Datacom learned in Europe will be applied. One rather disturbing omen has surfaced. Some people in the USA have started to refer to the DirecTv system as VideoCrypt rather than VideoGuard.

The Ho Lee Fook Hack

There is no such thing as coincidence or is there? On the day in 1993 that the film "Sneakers" was released on video I received an actual working hack for the scrambled Sky channels. The film "Sneakers" is about events surrounding a piece of equipment that can hack any cryptosystem. The piece of equipment that I received was essentially a chip that hacked the BSkyB VideoCrypt channels

The hack on the VideoCrypt system was labeled the "Ho Lee Fook" hack. The reason for this name is more to do with people's reaction to the hack rather than its origin. Very few people are sure as to where exactly the hack originated and those who are sure are not speaking.

The VideoCrypt system is the mainstay of the BSkyB satellite television empire. It is the means by which BSkyB makes its money from the subscribers. The basic theory is that they pay a subscription for the premium channels and they receive a smart card. This smart card, when inserted into the VideoCrypt decoder will allow the decoder to descramble the channels paid for. It is also possible for BSkyB to turn off the cards of those subscribers who have not paid.

Other channels using the VideoCrypt system were hit. The Adult Channel, JSTV and TV Asia were compromised as well. This meant that all of the channels using the VideoCrypt system as a fee gathering system lost control of the market in one fell swoop.

This is perhaps the most dangerous hack to have occurred on VideoCrypt. In effect it was a new smart card that gave access to all the Sky channels. Of course the problem for Sky was that it was not a genuine Sky card.

The pirate smart card was approximately sixteen millimetres longer than the official Sky card. It is a blue printed circuit with a single surface mount chip. There were five connector pads.

The standard check for a card of this nature is to look for a wafer from an official smart card. In the early days, a fairly common scam was to take the chip and connector pad from a valid Sky card, trim away the plastic and then put the chip in a DIL header. The DIL header would then be blobbed in a lump of black resin so that it looked like an IC.

The chip on the PCB was the real thing. There was no wafer underneath the body of the chip. The actual stubs of the chip die were just visible at the end of the chip. The chip was a PIC16C54. This was the EPROM version of the now commonplace PIC16C84.

Actually there were two different versions of the Ho Lee Fook hack. The card version was the later one. The first version was a replacement for the 8052 in the decoder. The official VideoCrypt name for the 8052 chip in the decoder is "The Verifier". This chip had to be removed and replaced with the Ho Lee Fook 8752 chip. The decoder then decoded the scrambled channels without the need for the BSkyB smart card. This was the exactly the thing that people had said could never happen - a cardless Sky decoder.

If it had been a direct clone, Sky would have been able to kill it over the air or would they? They were not able to kill the Ho Lee Fook cards by neutralising a specific card identity - the pirate smart cards had no card identity numbers. When they were reset, they returned a string of zeroes as their identity number.

There were of course more devastating implications here. The card only contained the data and algorithms necessary to descramble the signals.

A card that only contained enough information to descramble the signal would reduced VideoCrypt to the status of a system like SAVE. More than a few hackers were laughing as a result. The arrogance of News Datacom only inspired hackers. Here were these people with their new system making out that they were better than all who had come before them and indeed all that stood before them. Obviously they, having inhabited the sterile environment of a laboratory for too long, did not realise that the mindpower employed to hack the system was far greater than that employed to design the system.

The much vaunted Fiat Shamir Zero Knowledge Test was nowhere to be seen. If the ZKT had indeed been implemented properly then all of these pirate cards would have been knocked out.

According to the early theory on VideoCrypt, the smart card had to authenticate itself to the decoder and prove it was a genuine smart card. This was apparently just a load of waffle. If it was not then the Ho Lee Fook would definitely have been knocked out as it only held the hash function and key tables. Incidentally the same claims are being made in the USA about the DirecTv system.

The 07 Ho Lee Fook lasted from April 1993 to 18th May 1994. News Datacom tried to implement every electronic countermeasure that they could. The hackers defeated every one of them, typically within a few minutes. In the end News Datacom were left with little alternative other than a new smart card. When they introduced this new smart card it was hacked roughly a month after its introduction. News Datacom knocked out this hack but at the time of writing a new hack is being tested. It looks like things may be back to the old ECM - ECCM cycle.

The listing that follows this text is the listing for an actual Ho Lee Fook chip. The chip used is the PIC16C84. The PCB layout is given in the Smart Card Section. However it is only presented here as a reference. The algorithm used in this is the 07 algorithm.

The fact that the VideoCrypt system has been hacked once means that it can happen again. This pattern has been has been seen in hacks on other scrambling systems. The VideoCipher II system is one that immediately springs to mind.

The VideoCipher II system was billed as the most secure system yet devised. Within a few months, hackers had discovered that the decoder could be fooled into allowing access to all channels having only paid for one. This was the EPROM hack or as it was know the Musketeer hack. The parallel with Sky would be the Zener diode or Infinite Lives hack. VideoCipher II is now in its third incarnation. Perhaps VideoCrypt may go through a similar set of incarnations.

When VideoCrypt was launched, there was only a stand alone decoder for the system. The decoder was only supposed to have been used in the UK or Ireland. Of course this was a naieve assumption. These decoders were being shipped out to mainland Europe by the truck load.

The biggest mistake made by BSkyB and perhaps News Datacom was letting the decoders be integrated with receivers. This produced the IRD. It is a lot simpler to ship an IRD than a decoder. Whereas the decoder would be listed as such on Customs and Excise documentation, the IRD would only be listed as a receiver.

Every so often the press would be bombarded by press releases claiming that BSkyB in conjunction with the UK Customs had prevented yet another truck load of decoders from reaching Europe. It

was a particularly dull period in BSkyB's history considering that anyone in mainland Europe who wanted a VideoCrypt decoder could get one without any real problems.

This new hack could not have occurred at a worse time for BSkyB. It was busy trying to persuade new channels to come on to its low pay tier which launched in the September 1993.

JSTV is a high fee channel and costs about thirty pounds per month. Since it is aimed at Japanese business people in Europe, it is catering for a niche market and as such commands such a high fee. Perhaps it was this relatively small niche market that saved JSTV from being widely pirated.

The Adult Channel was the most vulnerable. The fact that they are marketing the smart cards on a yearly basis would imply that upgrading the cards would be a heavy financial burden. They are now totally hacked as the 96 byte key table is available on many BBSes throughout Europe.

The issue of new card batches for BSkyB channels occurs mainly in Spring or Autumn. A Summer launch of the new 08 cards would be have been unusual. Indeed the 08 card design had to be junked as it probably was little more than a change of code tables. BSkyB were eventually forced to issue an 09 card in February 1994. This was at least six months ahead of their own schedule.

The philosophy of VideoCrypt is that of the detachable secure controller. Basically what this means is that if the system is hacked then all that needs to be done to stop the hack is to issue a new card.

The effects on the confidence of present and prospective users of VideoCrypt is more difficult to gauge. The smart card is the core of the VideoCrypt system. Seeing it replaced by a pirate smart card contradicts every claim made in favour of VideoCrypt. It was not supposed to be possible. One thing is certain, channels will now have to look at a scrambling system as only being a temporary form of protection that has to be frequently updated. Failure to do so will be fatal.

```
  LIST P=16C84
  LIST C=132
  LIST N=55
  LIST F=INHX8M
  TITLE 'ISO_7816_INTERFACE_DEVICE'

;*****************************************************************************
;* MODULE :
;* INPUT PARAMETERS :
;* OUTPUT PARAMETERS :
;* DESCRIPTION : ISO 7816 INTERFACE DEVICE
;*****************************************************************************
  INCLUDE "PIC84V4.H"
  PAGE
  ORG PIC84
  GOTO MAIN
  ORG 004H
  RETFIE
;*****************************************************************************
ANSWER_TO_RESET_SEQUENCE ; ;
  ADDWF PC,SAME ; 1 ;
  RETLW 03FH ; 2 ;
  RETLW 0FAH ; 2 ;
  RETLW 011H ; 2 ;
  RETLW 025H ; 2 ;
  RETLW 000H ; 2 ;
  RETLW 000H ; 2 ;
  RETLW 001H ; 2 ;
  RETLW 0B0H ; 2 ;
  RETLW 002H ; 2 ;
  RETLW 000H ; 2 ;
  RETLW 000H ; 2 ;
  RETLW 04DH ; 2 ;
  RETLW 059H ; 2 ;
  RETLW 000H ; 2 ;
  RETLW 081H ; 2 ;
  RETLW 080H ; 2 ;
  ; ;
;*****************************************************************************
VALID_INSTRUCTIONS ; 1 ;
  ADDWF PC,SAME ; 1 ;WRITE_INSTRUCTIONS:
  RETLW 000H ; 2 ;DUMMY INSTRUCTION_CODE
  RETLW 070H ; 2 ;INSTRUCTION_CODE 0X70
  RETLW 078H ; 2 ;INSTRUCTION_CODE 0X78
  RETLW 07AH ; 2 ;INSTRUCTION_CODE 0X7A
  RETLW 07CH ; 2 ;INSTRUCTION_CODE 0X7C
```

```
   RETLW 07EH ; 2 ;INSTRUCTION_CODE 0X7E
   RETLW 082H ; 2 ;INSTRUCTION_CODE 0X82
   ; ;READ_INSTRUCTIONS:
   RETLW 072H ; 2 ;INSTRUCTION_CODE 0X72
   RETLW 074H ; 2 ;INSTRUCTION_CODE 0X74
   RETLW 076H ; 2 ;INSTRUCTION_CODE 0X76
   RETLW 080H ; 2 ;INSTRUCTION_CODE 0X80
;*******************************************************************************
STRING
   MOVLW 000H ; 1 ;
   SUBWF OSD_COUNT,WREG ; 1 ;
   BTFSS STATUS,Z ; 1 ;
   GOTO ANNOUNCE ; 1 ; IF ( OSD_COUNT == 00 )
   ; ;
   BTFSS FLAGS1,STR_HEADER ; 1 ;
   GOTO STRING1 ; 2 ;
   RETLW 000H ; 2 ; IF ( HEADER SENT ) RETURN (0)
STRING1
   BSF FLAGS1,STR_HEADER ; 1 ; IF FIRST TIME, RETURN (0X80)
   RETLW 080H ; 2 ; AND SET STR_HEADER
;---------------------------------------------
ANNOUNCE
   MOVLW 019H ; 1 ;
   ADDWF COUNTER,WREG ; 1 ;
   ADDWF PC,SAME ; 1 ;
   RETLW 0D8H ; 2 ;
   RETLW 'G' ; 2 ;
   RETLW 'O' ; 2 ;
   RETLW 'L' ; 2 ;
   RETLW 'D' ; 2 ;
   RETLW 'C' ; 2 ;
   RETLW 'A' ; 2 ;
   RETLW 'R' ; 2 ;
   RETLW 'D' ; 2 ;
   RETLW ' ' ; 2 ;
   RETLW '1' ; 2 ;
   RETLW '.' ; 2 ;
   RETLW '4' ; 2 ;
   RETLW 'C' ; 2 ;
   RETLW 'R' ; 2 ;
   RETLW 'Y' ; 2 ;
   RETLW 'P' ; 2 ;
   RETLW 'T' ; 2 ;
   RETLW 'M' ; 2 ;
   RETLW 'O' ; 2 ;
   RETLW 'D' ; 2 ;
   RETLW 'E' ; 2 ;
   RETLW ':' ; 2 ;
   RETLW '0' ; 2 ;
   MOVLW 00FH ; 1 ;
```

```
   ANDWF C_MODE,SAME ; 1 ;
   MOVF C_MODE,WREG ; 1 ;
   ADDLW '0' ; 1 ;
   RETURN ; 1 ;
;*****************************************************************************
DECIPHER_KEY
   ADDWF PC,SAME ; 1 ;
   RETLW 065H ; 2 ;
   RETLW 0E7H ; 2 ;
   RETLW 071H ; 2 ;
   RETLW 01AH ; 2 ;
   RETLW 0B4H ; 2 ;
   RETLW 088H ; 2 ;
   RETLW 0D7H ; 2 ;
   RETLW 076H ; 2 ;
   ; ;
   RETLW 028H ; 2 ;
   RETLW 0D0H ; 2 ;
   RETLW 04CH ; 2 ;
   RETLW 06EH ; 2 ;
   RETLW 086H ; 2 ;
   RETLW 08CH ; 2 ;
   RETLW 0C8H ; 2 ;
   RETLW 043H ; 2 ;
   ; ;
   RETLW 0A9H ; 2 ;
   RETLW 0ECH ; 2 ;
   RETLW 060H ; 2 ;
   RETLW 042H ; 2 ;
   RETLW 005H ; 2 ;
   RETLW 0F2H ; 2 ;
   RETLW 03DH ; 2 ;
   RETLW 01CH ; 2 ;
   ; ;
   RETLW 06CH ; 2 ;
   RETLW 0BCH ; 2 ;
   RETLW 0AFH ; 2 ;
   RETLW 0C3H ; 2 ;
   RETLW 02BH ; 2 ;
   RETLW 0B5H ; 2 ;
   RETLW 0DCH ; 2 ;
   RETLW 090H ; 2 ;
   ; ;
   RETLW 0F9H ; 2 ;
   RETLW 005H ; 2 ;
   RETLW 0EAH ; 2 ;
   RETLW 051H ; 2 ;
   RETLW 046H ; 2 ;
   RETLW 09DH ; 2 ;
   RETLW 0E2H ; 2 ;
```

```
   RETLW 060H ; 2 ;
   ; ;
   RETLW 070H ; 2 ;
   RETLW 052H ; 2 ;
   RETLW 067H ; 2 ;
   RETLW 026H ; 2 ;
   RETLW 061H ; 2 ;
   RETLW 049H ; 2 ;
   RETLW 042H ; 2 ;
   RETLW 009H ; 2 ;
   ; ;
   RETLW 050H ; 2 ;
   RETLW 099H ; 2 ;
   RETLW 090H ; 2 ;
   RETLW 0A2H ; 2 ;
   RETLW 036H ; 2 ;
   RETLW 00EH ; 2 ;
   RETLW 0FDH ; 2 ;
   RETLW 039H ; 2 ;

    PAGE

;*****************************************************************************

    ORG 0100H ; ;
MAIN
   MOVLW 07FH ; 1 ;
   OPTION ; 1 ; PULL UP'S ON PORT B ENABLE
   MOVLW 000H ; 1 ;
   MOVWF STATUS ; 1 ;
   MOVLW TRI_A_MASK ; 1 ;
   BSF STATUS,RP0 ; 1 ; PAGE SELECT
   MOVWF TRISA ; 1 ; SET DATA DIRECTION
   BCF STATUS,RP0 ; 1 ; PAGE SELECT
   MOVLW LATCH_A_MASK ; 1 ;
   MOVWF PORT_A ; 1 ; LATCHES LOW
   MOVLW TRI_B_MASK ; 1 ;
   BSF STATUS,RP0 ; 1 ; PAGE SELECT
   MOVWF TRISB ; 1 ; SET DATA DIRECTION
   BCF STATUS,RP0 ; 1 ; PAGE SELECT
   MOVLW LATCH_B_MASK ; 1 ;
   MOVWF COM_PORT ; 1 ;
   ; ;
   BCF FLAGS,CONVENTION ; 1 ;PROTOCOL IN INVERSE_CONVENTION
   BCF FLAGS,CHECKSUM_OK ; 1 ;CHECKSUM_OK = 0
   BCF FLAGS,DECODE_ON_WRITE ; 1 ;DECODE_ON_WRITE = 0
   CLRF FLAGS1 ; 1 ;
   CLRF WORK ; 1 ;
   ; ;
   MOVLW 006H ; 1 ;
   MOVWF OSD_COUNT ; 1 ;OSD = ON
```

```
   ; ;
   MOVLW C_MODE_EE_ADR ; 1 ; LOAD ADDRESS POINTER
   MOVWF EEADR ; 1 ;
   BSF STATUS,RP0 ; 1 ; PAGE 1
   BSF EECON1,EE_RD ; 1 ; RESTORE C_MODE
   BCF STATUS,RP0 ; 1 ; PAGE 0
   MOVF EEDATA,WREG ; 1 ;
   MOVWF C_MODE ; 1 ; SAVE DATA IN C_MODE
   ; ;
   CALL ANSWER_TO_RESET ; 1 ;ANSWER TO RESET
   ; ;
INFINITE_LOOP ; 1 ;
   BCF FLAGS,CHCKSUM_REQUEST ; 1 ;CHCKSUM_REQUEST = 0
   BCF FLAGS,DECODE_ON_READ ; 1 ;DECODE_ON_READ = 0
   BCF FLAGS,SEND_REG_B1 ; 1 ;SEND_REG_B1 = 0
   BCF FLAGS,STRING_REQUEST ; 1 ;STRING_REQUEST = 0
   BCF FLAGS1,STR_HEADER ; 1 ;STR_HEADER = 0
   BCF FLAGS1,READ_82 ; 1 ;READ_82 = 0
   BCF FLAGS1,A82_HEADER ; 1 ;A82_HEADER = 0
INSTRUCTION_LOOP ; ;
   MOVLW INSTRUCTION_CLASS ; 1 ;RECEIVE_POINTER = INSTRUCTION_CLASS
   MOVWF FSR ; 1 ;
   CALL RECEIVE_ISO_ASYNC ; 1 ;INSTRUCTION_CLASS = RECEIVE_ISO_ASYNC ( );
   BTFSS STATUS,C ; 1 ; IF ( ! C )
   GOTO INFINITE_LOOP ; 1 ; CONTINUE
   ; ;
   CALL RECEIVE_ISO_ASYNC ; 1 ;INSTRUCTION_CODE = RECEIVE_ISO_ASYNC ( );
   CALL RECEIVE_ISO_ASYNC ; 1 ;DUMMY1 = RECEIVE_ISO_ASYNC ( );
   DECF FSR,SAME ; 1 ;
   CALL RECEIVE_ISO_ASYNC ; 1 ;DUMMY1 = RECEIVE_ISO_ASYNC ( );
   CALL RECEIVE_ISO_ASYNC ; 1 ;COUNTER = RECEIVE_ISO_ASYNC ( );
   MOVLW 053H ; 1 ;
   SUBWF INSTRUCTION_CLASS,WREG ; 1 ;IF ( INSTRUCTION_CLASS ! = 0X53 )
   BTFSC STATUS,Z ;1/2; {
   GOTO INSTRUCTION_DECODING ; 2 ; SW1 = 0X6E;
   MOVLW 06EH ; 1 ; INSTRUCTION_CLASS INVALID
   GOTO TRANSMIT_SW1 ; 2 ; BREAK;
   ; ; }
INSTRUCTION_DECODING ; ;
   MOVLW 00AH ; 1 ;
   MOVWF REG_00 ; 1 ;
INSTR_DECODE_LOOP ; 1 ;FOR ( INDEX = 0X0A ; INDEX ; INDEX++ )
   MOVF REG_00,WREG ; 1 ; {
   CALL VALID_INSTRUCTIONS ; 1 ; IF ( INSTRUCTION_CODE ==
   SUBWF INSTRUCTION_CODE,WREG ; 1 ; VALID_INSTRUCTIONS [ INDEX ] )
   BTFSC STATUS,Z ; 1 ; {
   GOTO INSTRUCTION_VALID ; 1 ; GOTO INSTRUCTION_VALID;
   DECFSZ REG_00,SAME ; 1 ; }
   GOTO INSTR_DECODE_LOOP ; 1 ; }
```

PIC16C84 Listing-5

```
   MOVLW 06DH ; 1 ;INSTRUCTION_CODE NOT SUPPORTED
   GOTO TRANSMIT_SW1 ; 1 ;
   PAGE
INSTRUCTION_VALID ; ;
   MOVLW 007H ; 1 ;IF ( INDEX < 0X07 )
   SUBWF REG_00,WREG ; 1 ; GOTO WRITE_MESSAGE
   BTFSS STATUS,C ;1/2;ELSE
   GOTO WRITE_MESSAGE ; 2 ; GOTO READ_MESSAGE
   ; ;
READ_MESSAGE ; ;
   MOVLW 076H ; 1 ;
   SUBWF INSTRUCTION_CODE,WREG ; 1 ;
   BTFSS STATUS,Z ; 1 ;IF ( INSTRUCTION_CODE == 0X76 )
   GOTO READ_MESS1 ; 2 ;
   ; ;
   MOVLW 006H ; 1 ; OSD_TIME = 006*RECEIVE 74
   MOVWF OSD_COUNT ; 1 ; OSD = ON
   ; ;
   MOVLW 00FH ; 1 ;
   INCF C_MODE,SAME ; 1 ; INC C_MODE
   ANDWF C_MODE,SAME ; 1 ;
   MOVLW 009H ; 1 ; !!!!! 0...8 !!!! 8X=MULTICHANNEL
   SUBWF C_MODE,WREG ; 1 ;
   BTFSC STATUS,C ; 1 ;
   CLRF C_MODE ; 1 ;
   CALL WREE_C_MODE ; 1 ;
READ_MESS1 ; ;
   MOVLW 074H ; 1 ;
   SUBWF INSTRUCTION_CODE,WREG ; 1 ;
   BTFSS STATUS,Z ; 1 ;IF ( INSTRUCTION_CODE == 0X74 )
   GOTO READ_MESS2 ; 2 ;
   MOVLW 000H ; 1 ; IF ( OSD_COUNT != 0 )
   SUBWF OSD_COUNT,WREG ; 1 ;
   BTFSS STATUS,Z ; 1 ;
   DECFSZ OSD_COUNT,SAME ; 1 ; OSD_COUNT--;
READ_MESS2
   MOVLW 074H ; 1 ;
   SUBWF INSTRUCTION_CODE,WREG ; 1 ;
   BTFSS STATUS,Z ; 1 ;IF ( INSTRUCTION_CODE == 0X74 )
   GOTO TRANSMIT_PROCEDURE_BYTE ; 2 ;
   BSF FLAGS,DECODE_ON_READ ; 1 ; DECODE_ON_READ = 1;
   BSF FLAGS,DECODE_ON_WRITE ; 1 ; DECODE_ON_WRITE = 1;
   BSF FLAGS,CHCKSUM_REQUEST ; 1 ; CHCKSUM_REQUEST = 1;
   BCF FLAGS,CHECKSUM_OK ; 1 ; CHECKSUM_OK = 0;
TRANSMIT_PROCEDURE_BYTE ; ;
   MOVF INSTRUCTION_CODE,WREG ; 1 ;ACCU = INSTRUCTION_CODE
   CALL TRANSMIT_ISO_ASYNC ; 1 ;SEND INSTRUCTION_CODE FOR ACKNOWL-
   EDGE
   CLRF CHECKSUM ; 1 ;CHECKSUM = 0
```

```
    PAGE
READ_MESSAGE_LOOP_1 ; ;FOR (COUNTER=0X20;COUNTER;COUNTER--)
   ; ; {
   MOVLW INSTRUCTION_CLASS ; 1 ;
   MOVWF FSR ; 1 ;
   CALL RECEIVE_ISO_ASYNC ; 1 ; INSTRUCTION_CLASS = RECEIVE_ISO_ASYNC ( );
   MOVF READ_BYTE,WREG ; 1 ;
   MOVWF INSTRUCTION_CODE ; 1 ; INSTRUCTION_CODE = READ_BYTE
   BTFSS FLAGS,DECODE_ON_READ ;1/2; IF ( ! DECODE_ON_READ )
   GOTO CONTINUE1 ; 2 ; BREAK;
   MOVLW 006H ; 1 ; IF ( COUNTER > 0X05 )
   SUBWF COUNTER,WREG ; 1 ; {
   BTFSS STATUS,C ;1/2;
   GOTO CONTINUE ; 2 ;
   CALL RECEIVE_ISO_ASYNC ; 1 ; INSTRUCTION_CODE = RECEIVE_ISO_ASYNC ( );
   DECF COUNTER,SAME ; 1 ;
   CALL RECEIVE_ISO_ASYNC ; 1 ; DUMMY1 = RECEIVE_ISO_ASYNC ( );
   DECF COUNTER,SAME ; 1 ;
   BSF FLAGS,INC_REQUEST ; 1 ; INCREMENT_REQUEST = 1
   MOVLW 01EH ; 1 ; IF ( COUNTER == 0X1E )
   SUBWF COUNTER,WREG ; 1 ; {
   BTFSC STATUS,Z ;1/2; CHECK_1 ( );
   CALL CHECK_1 ; 2 ; }
   MOVLW 01BH ; 1 ; IF ( COUNTER == 0X1B )
   SUBWF COUNTER,WREG ; 1 ; {
   BTFSC STATUS,Z ;1/2; CHECK_2 ( );
   CALL CHECK_2 ; 2 ; }
   MOVLW 018H ; 1 ; IF ( COUNTER == 0X18 )
   SUBWF COUNTER,WREG ; 1 ; {
   BTFSC STATUS,Z ;1/2; CHECK_3 ( );
   CALL CHECK_3 ; 2 ; }
   MOVLW 003H ; 1 ;
   CALL DECIPHER_N_BYTE ; 2 ; DECIPHER_3_BYTE;
   CLRF REG_47 ; 1 ; REG_47 = 0X00
   GOTO CONTINUE1 ; 2 ; }
CONTINUE ; ; ELSE
   MOVF REG_47,WREG ; 1 ; {
   MOVWF INSTRUCTION_CLASS ; 1 ;     |-->INSTR_CLASS-->REG_47->--|
   MOVF INSTRUCTION_CODE,WREG ; 1 ;|----------------<------------------------|
   MOVWF REG_47 ; 1 ; REG_47 = INSTRUCTION_CLASS
   DECF COUNTER,WREG ; 1 ;
   BTFSC STATUS,Z ;1/2; IF ( COUNTER != 0X01 )
   GOTO CONTINUE1 ; 2 ; {
   BCF FLAGS,INC_REQUEST ; 1 ; INCREMENT_REQUEST = 0
   MOVLW 002H ; 1 ; DECIPHER 2 BYTE
   CALL DECIPHER_N_BYTE ; 2 ;
   INCF REG_B1_POINTER,SAME ; 1 ; REG_B1_POINTER ++;
   MOVLW 007H ; 1 ; REG_B1_POINTER &= 0X07;
   ANDWF REG_B1_POINTER,SAME ; 1 ; }
```

```
CONTINUE1 ; ; }
   DECFSZ COUNTER,SAME ; 1 ; }
   GOTO READ_MESSAGE_LOOP_1 ; 1 ;IF ( CHCKSUM_REQUEST )
   BTFSS FLAGS,CHCKSUM_REQUEST ;1/2; {
   GOTO END_OF_MESSAGE ; 2 ; IF ( CHECKSUM == 0X00 )
   MOVF CHECKSUM,SAME ; 1 ; {
   BTFSC STATUS,Z ;1/2; CHECKSUM_OK = 1;
   BSF FLAGS,CHECKSUM_OK ; 1 ; }
   GOTO END_OF_MESSAGE ; 1 ; }

     PAGE

WRITE_MESSAGE ; 1 ;
   MOVF INSTRUCTION_CODE,WREG ; 1 ;ACCU = INSTRUCTION_CODE
   CALL TRANSMIT_ISO_ASYNC ; 1 ;SEND INSTRUCTION_CODE FOR ACKNOWL-
   EDGE
   MOVLW 078H ; 1 ;IF ( INSTRUCTION_CODE == 0X78 )
   SUBWF INSTRUCTION_CODE,WREG ; 1 ; {
   BTFSS STATUS,Z ;1/2;
   GOTO WRITE_STRING ; 2 ;
   BSF FLAGS,SEND_REG_B1 ; 1 ; SEND_REG_B1 = 1
   MOVF REG_47,WREG ; 1 ; DECIPHER WITH REG_47
   MOVWF INSTRUCTION_CLASS ; 1 ;
   MOVLW 040H ; 1 ;
   BTFSC FLAGS,DECODE_ON_WRITE ;1/2;
   CALL DECIPHER_BYTE ; 2 ; DECIPHER_64_BYTE;
   BCF FLAGS,DECODE_ON_WRITE ; 1 ;
WRITE_STRING ; ; }
   MOVLW 07AH ; 1 ;
   SUBWF INSTRUCTION_CODE,WREG ; 1 ;
   BTFSC STATUS,Z ; 1 ;
   BSF FLAGS,STRING_REQUEST ; 1 ;
   COMF COUNTER,SAME ; 1 ;2'S COMPLEMENT COUNTER
   INCF COUNTER,SAME ; 1 ;
WRITE_MESSAGE_LOOP ; ;DO
   CLRW ; 1 ; {
   BTFSC FLAGS,STRING_REQUEST ;1/2;
   CALL STRING ; 2 ; STRING_OUTPUT
   BTFSC FLAGS,CHECKSUM_OK ;1/2;
   BTFSS FLAGS,SEND_REG_B1 ;1/2;
   GOTO OUTPUT ; 2 ;
   MOVLW ARRAY_REG_B1+8 ; 1 ;
   ADDWF COUNTER,WREG ; 1 ;
   MOVWF FSR ; 1 ;
   MOVF IND0,WREG ; 1 ;
OUTPUT ; ;
   CALL TRANSMIT_ISO_ASYNC ; 2 ; SEND_SINGLE_BYTE;
   INCFSZ COUNTER,SAME ;1/2; }
   GOTO WRITE_MESSAGE_LOOP ; 2 ;WHILE ( -- COUNTER );
   ; ;
```

```
END_OF_MESSAGE ; 1 ;END_OF_MESSAGE_SEQUENCE
   MOVLW 090H ; 1 ;SW1 = 0X90
TRANSMIT_SW1
   CALL TRANSMIT_ISO_ASYNC ; 1 ;TRANSMIT SW1
   MOVLW 000H ; 1 ;
   CALL TRANSMIT_ISO_ASYNC ; 1 ;TRANSMIT SW2
   ; ;
   GOTO INFINITE_LOOP ; 1 ;
   ; ;
    PAGE
;*****************************************************************************
;* MODULE : ANSWER_TO_RESET
;* USING : REG_03,REG_04
;* INPUT PARAMETERS :
;* OUTPUT PARAMETERS :
;* DESCRIPTION :
;*****************************************************************************
ANSWER_TO_RESET
   CLRF REG_05 ; 1 ;
ANSWER_TO_RESET_LOOP ; 1 ;
   MOVF REG_05,WREG ; 1 ;
   CALL ANSWER_TO_RESET_SEQUENCE; 2 ;
   CALL TRANSMIT_ISO_ASYNC ; 2 ;
   INCF REG_05,SAME ; 1 ;
   BTFSS REG_05,4 ;1/2;
   GOTO ANSWER_TO_RESET_LOOP ; 1 ;
   RETLW 0 ; 2 ;
    PAGE
;*****************************************************************************
;* MODULE : CHECK_1
;* USING : REG_00,REG_04,REG_05
;* INPUT PARAMETERS :
;* OUTPUT PARAMETERS :
;* DESCRIPTION :
;*****************************************************************************
CHECK_1
   CLRF REG_B1_POINTER ; 1 ;REG_B1_POINTER = 0X00
   CLRF DEC_KEY_POINTER ; 1 ;DECIPHER_KEY_POINTER = 0X00
   BCF FLAGS1,DATA_HEAD ; 1 ;DATA_HEADER = FALSE
   BTFSC INSTRUCTION_CLASS,4 ; 1 ; TEST IF XXX1 XXXX
```

```
   BSF FLAGS1,DATA_HEAD ; 1 ;
   MOVLW 0E8H ; 1 ;
   SUBWF INSTRUCTION_CLASS,WREG ; 1 ;
   ANDLW 0EFH ; 1 ;MASK 0XE8 OR 0XF8
   BTFSS STATUS,Z ;1/2;IF ( ARRAY_REG_28 [ 0 ] != 0XE8 )
   BCF FLAGS,DECODE_ON_READ ; 1 ; DECODE_ON_READ = 0
   BTFSS STATUS,Z ;1/2;IF ( ARRAY_REG_28 [ 0 ] != 0XE8 )
   BCF FLAGS,DECODE_ON_WRITE ; 1 ; DECODE_ON_WRITE = 0;
   CALL CLEAR_ARRAY_REG_B1 ; 2 ;CLEAR ARRAY REG_B1
   MOVLW 033H ; 1 ;IF ( ARRAY_REG_28 [ 1 ] < 0X33 )
   SUBWF INSTRUCTION_CODE,WREG ; 1 ; DECIPHER_KEY_POINTER = 0X00;
   CLRW ; 1 ;
   BTFSC STATUS,C ;1/2;ELSE
   MOVLW 008H ; 1 ; DECIPHER_KEY_POINTER = 0X08;
   MOVWF DEC_KEY_POINTER ; 1 ;
   MOVLW 03BH ; 1 ;IF ( ARRAY_REG_28 [ 1 ] < 0X3B )
   SUBWF INSTRUCTION_CODE,WREG ; 1 ; DECIPHER_KEY_POINTER = 0X08;
   MOVF DEC_KEY_POINTER,WREG ; 1 ;ELSE
   BTFSC STATUS,C ;1/2; DECIPHER_KEY_POINTER = 0X18;
   MOVLW 018H ; 1 ;
   MOVWF DEC_KEY_POINTER ; 1 ;
   RETLW 000H ; 2 ;

    PAGE
;*****************************************************************************
;* MODULE : CHECK_2
;* USING : REG_00,REG_04,REG_05
;* INPUT PARAMETERS :
;* OUTPUT PARAMETERS :
;* DESCRIPTION :
;*****************************************************************************
CHECK_2
   BTFSC FLAGS1,DATA_HEAD ; 1 ;TEST IF DATA_HEADER == 0XF8
   GOTO CHECK_ZERO_END ; 2 ; THEN SKIP TEST AND DECODE
   MOVF INSTRUCTION_CODE,WREG ; 1 ;W = ARRAY_REG_28 [ 4 ]
   IORWF DUMMY1,WREG ; 1 ;W |= ARRAY_REG_28 [ 5 ]
   BTFSS STATUS,Z ;1/2;
   GOTO CHECK_ZERO_END ; 2 ;
   CALL CLEAR_ARRAY_REG_B1 ; 2 ;
   MOVLW 001H ; 1 ;
   MOVWF ARRAY_REG_B1 ; 1 ;
   BCF FLAGS,DECODE_ON_READ ; 1 ;
   BCF FLAGS,DECODE_ON_WRITE ; 1 ; DECODE_ON_WRITE = 0;
   CHECK_ZERO_END ; ;
   RETLW 000H ; 2 ;

    PAGE
```

```
;*******************************************************************************
;* MODULE : CHECK_3
;* USING : REG_00,REG_04,REG_05
;* INPUT PARAMETERS :
;* OUTPUT PARAMETERS :
;* DESCRIPTION :
;*******************************************************************************
CHECK_3
   MOVLW TRI_B_MASK ; 1 ;
   BSF STATUS,RP0 ; 1 ; PAGE SELECT
   MOVWF TRISB ; 1 ; SET DATA DIRECTION
   BCF STATUS,RP0 ; 1 ; PAGE SELECT
   MOVLW LATCH_B_MASK ; 1 ;
   MOVWF COM_PORT ; 1 ;
   BTFSC SOLDPO2,SOLDPI2 ; 1 ; CHECK SOLDER 2
   GOTO CHECK_31 ; 2 ; IF CLOSED -> == 0
   MOVLW 00FH ; 1 ; TEST FOR ID = 8
   ANDWF INSTRUCTION_CLASS,WREG ; 1 ;
   MOVWF WORK ; 1 ;
   MOVLW 007H ; 1 ;
   ANDWF WORK,WREG ; 1 ; IF ( ID != 0X08 && ID != 0X00 )
   BTFSC STATUS,Z ;1/2; GO_ON
   GOTO WRONG_3 ; 2 ;
CHECK_31
   SWAPF C_MODE,WREG ; 1 ; MASK ID
   ANDWF INSTRUCTION_CLASS,WREG ; 1 ;
   BTFSC STATUS,Z ;1/2;
   GOTO CHECK_3_END ; 2 ;
WRONG_3
   CALL CLEAR_ARRAY_REG_B1 ; 2 ;
   RCF FLAGS,DECODE_ON_READ ; 1 ;
   BCF FLAGS,DECODE_ON_WRITE ; 1 ; DECODE_ON_WRITE = 0;
CHECK_3_END ; ;
   RETLW 000H ; 2 ;
    PAGE
```

```
;*******************************************************************************
;* MODULE : CLEAR_ARRAY_REG_B1
;* USING :
;* INPUT PARAMETERS :
;* OUTPUT PARAMETERS :
;* DESCRIPTION :
;*******************************************************************************
CLEAR_ARRAY_REG_B1
   CLRF ARRAY_REG_B1 ; 1 ;ARRAY_REG_B1 [ 0 ] = 0
   CLRF ARRAY_REG_B1+1 ; 1 ;ARRAY_REG_B1 [ 1 ] = 0
   CLRF ARRAY_REG_B1+2 ; 1 ;ARRAY_REG_B1 [ 2 ] = 0
   CLRF ARRAY_REG_B1+3 ; 1 ;ARRAY_REG_B1 [ 3 ] = 0
   CLRF ARRAY_REG_B1+4 ; 1 ;ARRAY_REG_B1 [ 4 ] = 0
   CLRF ARRAY_REG_B1+5 ; 1 ;ARRAY_REG_B1 [ 5 ] = 0
   CLRF ARRAY_REG_B1+6 ; 1 ;ARRAY_REG_B1 [ 6 ] = 0
   CLRF ARRAY_REG_B1+7 ; 1 ;ARRAY_REG_B1 [ 7 ] = 0
   RETLW 000H ; 2 ;
    PAGE
;*******************************************************************************
;* MODULE : DECIPHER_N_BYTE
;* USING : REG_00,REG_01,REG_02,REG_03,FSR
;* INPUT PARAMETERS :
;* OUTPUT PARAMETERS :
;* DESCRIPTION :
;*******************************************************************************
   PAGE
DECIPHER_N_BYTE
   BTFSS FLAGS,DECODE_ON_READ ;1/2;
   RETLW 000H ; 2 ;
DECIPHER_BYTE ; ;
   MOVWF REG_03 ; 1 ;N IN W
   MOVLW INSTRUCTION_CLASS ; 1 ;PLAINTEXT_POINTER = INSTRUCTION_CLASS
   MOVWF REG_02 ; 1 ;REG_02 = PLAINTEXT_POINTER
DECIPHER_LOOP ; ;DO
   MOVF REG_02,WREG ; 1 ; {
   MOVWF FSR ; 1 ; SFR = PLAINTEXT_POINTER
   MOVF IND0,WREG ; 1 ; W = PLAINTEXT_BYTE
   MOVWF REG_00 ; 1 ; SAVE PLAINTEXT_BYTE;
   MOVLW ARRAY_REG_B1 ; 1 ; W = & ARRAY_REG_B1 [ 0 ]
   ADDWF REG_B1_POINTER,WREG ; 1 ; W = W + REG_B1_POINTER;
   MOVWF FSR ; 1 ; FSR = REG_B1_POINTER;
   INCF REG_B1_POINTER,SAME ; 1 ; REG_B1_POINTER ++;
   MOVLW 007H ; 1 ;
```

```
ANDWF REG_B1_POINTER,SAME ; 1 ; REG_B1_POINTER &= 0X07;
MOVF REG_00,WREG ; 1 ; RESTORE_PLAINTEXT_BYTE;
XORWF IND0,SAME ; 1 ; ARRAY_REG_B1 [ FSR ] ^= PLAINTEXT_BYTE;
SWAPF IND0,WREG ; 1 ; W = SWAP ( ARRAY_REG_B1 [ FSR ] );
ANDLW 00FH ; 1 ; W = W & 0X0F;
ADDWF DEC_KEY_POINTER,WREG ; 1 ; W = W + DECIPHER_KEY_POINTER;
CALL DECIPHER_KEY ; 2 ; W = DECIPHER_KEY [ W ];
MOVWF REG_01 ; 1 ; SAVE W TEMPORARILY
MOVF IND0,WREG ; 1 ; W = ARRAY_REG_B1 [ FSR ];
ANDLW 00FH ; 1 ; W = W & 0X0F;
IORLW 010H ; 1 ; W = W + 0X10;
ADDWF DEC_KEY_POINTER,WREG ; 1 ; W = W + DECIPHER_KEY_POINTER;
CALL DECIPHER_KEY ; 1 ; W = DECIPHER_KEY [ W ];
ADDWF REG_01,SAME ; 1 ; REG_01 = W + REG_01
COMF REG_01,SAME ; 1 ; REG_01 = ~ REG_01;
MOVF REG_01,WREG ; 1 ; W = REG_01
ADDWF REG_01,SAME ; 1 ; REG_01 = REG_01 * 0X02;
BTFSC STATUS,C ;1/2;
INCF REG_01,SAME ; 1 ; REG_01 += C;
MOVF REG_00,WREG ; 1 ; W = REG_00; ( PLAINTEXT_BYTE )
ADDWF REG_01,SAME ; 1 ; REG_01 += W;
MOVF REG_01,WREG ; 1 ; W = REG_01
ADDWF REG_01,SAME ; 1 ; REG_01 = REG_01 * 0X02;
BTFSC STATUS,C ;1/2;
INCF REG_01,SAME ; 1 ; REG_01 += C;
SWAPF REG_01,SAME ; 1 ; REG_01 = SWAP ( REG_01 );
MOVLW ARRAY_REG_B1 ; 1 ; W = & ARRAY_REG_B1 [ 0 ]
ADDWF REG_B1_POINTER,WREG ; 1 ; W = REG_B1_POINTER
MOVWF FSR ; 1 ; FSR = REG_B1_POINTER
MOVF REG_01,WREG ; 1 ; W = REG_01
XORWF IND0,SAME ; 1 ; ARRAY_REG_B1 [ FSR ] ^= REG_01;
BTFSC FLAGS,INC_REQUEST ;1/2; IF ( INCREMENT_REQUEST )
INCF REG_02,SAME ; 1 ; {
DECFSZ REG_03,SAME ;1/2; REG_02 ++
GOTO DECIPHER_LOOP ; 2 ; }
RETLW 000H ; 2 ; }
;?38;WHILE ( -- REG_03 );
```

PAGE

```
;*****************************************************************************
;* MODULE :
;* USING : REG_00,REG_01,REG_02,REG_03(SEND_BYTE) PSW
;* INPUT PARAMETERS :
;* OUTPUT PARAMETERS :
;* DESCRIPTION :
;*XYZ
;*****************************************************************************
;ASYNCHRONOUS COMMUNICATION CARD --> CONTROLLER
;*********************************************
; BIT TRANSMIT_ISO_ASYNC ( UNSIGNED CHAR SEND_BYTE )
TRANSMIT_ISO_ASYNC
   BCF COM_PORT,ISOTXD ; 1 ;LOW ----> TXD LATCH
   MOVWF SEND_BYTE ; 1 ;
   MOVLW 00FH ; 1 ;RETRY_COUNTER (BYTE) = 15
   MOVWF REG_02 ; 1 ;
TRANSMIT_BYTE ; ;
   MOVLW 006H ; 1 ;GUARDTIME = 5
   MOVWF REG_01 ; 1 ;
GUARDTIME_DELAY ; ;
   MOVLW 01EH ; 1 ;FOR (COUNTER1 = 0X06;COUNTER1 != 0;COUNTER1--)
   MOVWF REG_00 ; 1 ; {
BIT_DELAY ; ;
   DECFSZ REG_00,SAME ; ; FOR (COUNTER = 0X1E;COUNTER != 0;COUNTER--);
   GOTO BIT_DELAY ;?89;
   DECFSZ REG_01,SAME ; ;
   GOTO GUARDTIME_DELAY ;?94;
   ; ; }? GUARDTIME * 94 - 1 [CYCLES]
   MOVLW 009H ; 1 ;BIT_COUNTER = 0X09
   MOVWF REG_01 ; 1 ;
   CLRF PSW ; 1 ;PARITY CALCULATE REGISTER
   BTFSS FLAGS,CONVENTION ;1/2;IF ( INVERSE_CONVENTION )
   ; ; {
   COMF SEND_BYTE,SAME ; 1 ; COMPLEMENT SEND_BYTE
   ; ; }
   BTFSS FLAGS,CONVENTION ;1/2;IF ( INVERSE_CONVENTION )
   ; ; {
   INCF PSW,SAME ; 1 ; COMPLEMENT PARITY
   ; ; }
   BCF STATUS,C ; 1 ;PREPARE STARTBIT
   GOTO BIT_OUTPUT ; 2 ;STARTBIT --> I/O
   ; ;FOR ( ;BIT_COUNTER != 0;BIT_COUNTER-- )
TRANSMIT_BIT ; ; {
   BTFSC FLAGS,CONVENTION ;1/2;
```

```
   RRF SEND_BYTE,SAME ; 1 ; DIRECT_CONVENTION : ROTATE RIGHT
   BTFSS FLAGS,CONVENTION ;1/2;
   RLF SEND_BYTE,SAME ; 1 ; INVERSE_CONVENTION : ROTATE LEFT
BIT_OUTPUT ; ;
   BTFSC STATUS,C ;1/2;
   INCF PSW,SAME ; 1 ; UPDATE_PARITY
   MOVLW TRI_B_MASK & 0FFH ; 1 ; TXD = INPUT ( TRISTATE )
   BTFSS STATUS,C ;1/2; OR
   MOVLW TRI_B_MASK & 0FEH ; 1 ; TXD = OUTPUT ( ACTIVE LOW )
   BSF STATUS,RP0 ; 1 ; PAGE SELECT
   MOVWF TRISB ; 1 ; SET DATA DIRECTION
   BCF STATUS,RP0 ; 1 ; PAGE SELECT
   MOVLW 019H ; 1 ;
   MOVWF REG_00 ; 1 ;
SEND_DATA_BIT_DELAY ;?14;
   DECFSZ REG_00,SAME ; ; FOR (COUNTER = 0X19;COUNTER != 0;COUNTER--);
   GOTO SEND_DATA_BIT_DELAY ;?74;
   NOP ; 1 ;
   NOP ; 1 ;
   DECFSZ REG_01,SAME ;1/2;
   GOTO TRANSMIT_BIT ; 2 ; }LOOP_CYCLE_TIME : 93 CYCLES
   MOVLW 002H ; 1 ;
   MOVWF REG_00 ; 1 ;
SEND_LAST_BIT_DELAY ; ;?83 AFTER OUTPUT OF LAST DATA_BIT
   DECFSZ REG_00,SAME ; ;FOR (COUNTER = 0X02;COUNTER != 0;COUNTER--);
   GOTO SEND_LAST_BIT_DELAY ;?05;
   MOVLW TRI_B_MASK & 0FFH ; 1 ; TXD = INPUT ( TRISTATE )
   BTFSS PSW,PARITY ;1/2; OR
   MOVLW TRI_B_MASK & 0FEH ; 1 ; TXD = OUTPUT ( ACTIVE LOW )
   BSF STATUS,RP0 ; 1 ; PAGE SELECT
   MOVWF TRISB ; 1 ; SET DATA DIRECTION
   BCF STATUS,RP0 ; 1 ; PAGE SELECT
   MOVLW 01DH ; 1 ;
   MOVWF REG_00 ; 1 ;
SEND_PARITY_DELAY ; ;
   DECFSZ REG_00,SAME ; ;FOR (COUNTER = 0X19;COUNTER != 0;COUNTER--);
   GOTO SEND_PARITY_DELAY ;?86;
   NOP ; 1 ;?90 AFTER OUTPUT OF PARITY
   MOVLW TRI_B_MASK & 0FFH ; 1 ; RB.0 = INPUT ( TRISTATE )
   BSF STATUS,RP0 ; 1 ; PAGE SELECT
   MOVWF TRISB ; 1 ; SET DATA DIRECTION
   BCF STATUS,RP0 ; 1 ; PAGE SELECT
   MOVLW 019H ; 1 ;
   MOVWF REG_00 ; 1 ;
SEND_STOPBIT_DELAY ; ;
   DECFSZ REG_00,SAME ; ;FOR (COUNTER = 0X19;COUNTER != 0;COUNTER--);
   GOTO SEND_STOPBIT_DELAY ;?74;
   BTFSC COM_PORT,ISOTXD ;1/2;?78 AFTER OUTPUT OF STOPBIT
```

```
   GOTO TRANSMIT_END ; 2 ;---> SAMPLE STOPBIT FOR PARITY_ERROR
   DECFSZ REG_02,SAME ;1/2;
   GOTO TRANSMIT_BYTE ; 2 ;
   BCF STATUS,C ; 1 ;PARITY_ERROR
   RETLW 0 ; 2 ;
   ; ;
TRANSMIT_END ; ;
   BSF STATUS,C ; 1 ;
   RETLW 0 ; 2 ;
; END OF _TRANSMIT_ISO_ASYNC

    PAGE
;*****************************************************************************
;* MODULE :
;* USING : REG_00,REG_01,REG_02,REG_03(READ_BYTE),PSW
;* INPUT PARAMETERS :
;* OUTPUT PARAMETERS :
;* DESCRIPTION :
;*****************************************************************************
;ASYNCHRONOUS COMMUNICATION CARD <-- CONTROLLER
;***********************************************
; BIT RECEIVE_ISO_ASYNC ( UNSIGNED CHAR IDATA *READ_BYTE )
RECEIVE_ISO_ASYNC
   BCF COM_PORT,ISOTXD ; 1 ;LOW ----> TXD LATCH
   MOVLW 00FH ; 1 ;
   MOVWF REG_02 ; 1 ;REPEAT_COUNTER = 15
RECEIVE_BYTE
   MOVLW 032H ; 1 ;WORK_WAITING_TIME P16C84 :
   MOVWF REG_01 ; 1 ;( ( 7 * 255 ) + 9 ) * 50 [CYCLES]
   CLRF REG_00 ; 1 ;( = 89700 CYCLES = 102,51 MS AT 3.500 MHZ )
SAMPLE_START_BIT ; ;
   BTFSS COM_PORT,ISORXD ;1/2;BEGIN_OF_START_BIT (POSITIVE_LOGIC)
   BTFSC COM_PORT,ISORXD ;1/2;
   GOTO STARTBIT_LOOP ; 2 ;
   GOTO STARTBIT_FOUND ; 2 ;
STARTBIT_LOOP ; ;
   DECFSZ REG_00,SAME ;1/2;
   GOTO SAMPLE_START_BIT ; 2 ;
   DECFSZ REG_01,SAME ;1/2;
   GOTO SAMPLE_START_BIT ; 2 ;
   GOTO READ_ERROR ; 2 ;
STARTBIT_FOUND ; ;?05 AFTER BEGIN OF STARTBIT
   MOVLW 008H ; 1 ;BIT_COUNTER = 0X08
   MOVWF REG_01 ; 1 ;
```

```
   CLRF IND0 ; 1 ;SHIFT_REGISTER = 0X00
   CLRF PSW ; 1 ;
   MOVLW 029H ; 1 ;
   MOVWF REG_00 ; 1 ;WAIT FOR END_OF_STARTBIT:
STARTBIT_DELAY ; ;
   DECFSZ REG_00,SAME ; ;FOR ( COUNTER = 0X29;COUNTER != 0X00;COUNTER-- );
   GOTO STARTBIT_DELAY ;?122;
   ; ;?133 AFTER BEGIN OF STARTBIT
   PAGE
   ; ;?133 AFTER BEGIN OF STARTBIT
RECEIVE_BIT ; ;READ 8 DATA_BITS:
   CLRF REG_00 ; 1 ;FOR ( ;BIT_COUNTER != 0X00;BIT_COUNTER-- )
   BTFSS FLAGS,CONVENTION ;1/2; {
   BSF REG_00,1 ; 1 ; ?136 AFTER BEGIN OF STARTBIT
   BTFSC COM_PORT,ISORXD ;1/2; SAMPLE I/O (DATA_BIT_N FIRST SAMPLE)
   INCF REG_00,SAME ; 1 ; ( 44 CYCLES AFTER BEGIN OF DATA_BIT_N)
   BTFSC COM_PORT,ISORXD ;1/2; SAMPLE I/O (DATA_BIT_N 2ND SAMPLE)
   INCF REG_00,SAME ; 1 ;
   BTFSC COM_PORT,ISORXD ;1/2; SAMPLE I/O (DATA_BIT_N 3RD SAMPLE)
   INCF REG_00,SAME ; 1 ;
   BTFSC REG_00,1 ;1/2;
   INCF PSW,SAME ; 1 ;
   BCF STATUS,C ; 1 ;
   BTFSC REG_00,1 ;1/2;
   BSF STATUS,C ; 1 ;
   BTFSC FLAGS,CONVENTION ;1/2;
   RRF IND0,SAME ; 1 ; ROTATE ACCU RIGHT THROUGH C
   BTFSS FLAGS,CONVENTION ;1/2;
   RLF IND0,SAME ; 1 ; ROTATE ACCU LEFT THROUGH C
   MOVLW 017H ; 1 ;
   MOVWF REG_00 ; 1 ;
READ_DATA_BIT_DELAY ;?20;
   DECFSZ REG_00,SAME ; ; FOR ( COUNTER = 0X12;COUNTER != 0X00;COUNTER--
   );
   GOTO READ_DATA_BIT_DELAY ;?68;
   NOP ; 1 ;
   NOP ; 1 ;
   DECFSZ REG_01 ;1/2;
   GOTO RECEIVE_BIT ; 2 ; }LOOP_CYCLE_TIME : 93 CYCLES
   CLRF REG_00 ; 1 ;
   BTFSS FLAGS,CONVENTION ;1/2;
   BSF REG_00,SAME ; 1 ;READ PARITY_BIT:
   NOP ; 1 ;?92 AFTER 1ST SAMPLE OF LAST DATA_BIT
   BTFSC COM_PORT,ISORXD ;1/2;SAMPLE I/O (PARITY_BIT FIRST SAMPLE)
   INCF REG_00,SAME ; 1 ;(44 CYCLES AFTER BEGIN OF PARITY_BIT)
   BTFSC COM_PORT,ISORXD ;1/2;SAMPLE I/O (PARITY_BIT 2ND SAMPLE)
   INCF REG_00,SAME ; 1 ;
   BTFSC COM_PORT,ISORXD ;1/2;SAMPLE I/O (PARITY_BIT 3RD SAMPLE)
   INCF REG_00,SAME ; 1 ;
```

```
   BTFSS PSW,PARITY ;1/2;ODD :IF(PSW.PARITY && !ISORXD) -> PARITY_ERROR
   COMF REG_00,SAME ; 1 ;EVEN:IF(!PSW.PARITY && ISORXD) -> PARITY_ERROR
   BTFSS REG_00,1 ;1/2;
   GOTO PARITY_ERROR ; 2 ;
   MOVLW 038H ; 1 ;
   MOVWF REG_00 ; 1 ;
READ_STOPBIT_DELAY ; ;
   DECFSZ REG_00,SAME ; ;FOR ( COUNTER = 0X13;COUNTER != 0X00;COUNTER-- );
   GOTO READ_STOPBIT_DELAY ;?167;
   MOVF IND0,WREG ; 1 ;
   MOVWF READ_BYTE ; 1 ;
   ADDWF CHECKSUM,SAME ; 1 ;CHECKSUM + = *FSR
   INCF FSR ; 1 ;
   BSF STATUS,C ; 1 ;
   RETLW 0 ; 2 ;?185 AFTER 1ST SAMPLE OF PARITY

    PAGE
PARITY_ERROR ; ;?10 AFTER 1ST SAMPLE OF PARITY
   MOVLW 018H ; 1 ;(54 CYCLES AFTER BEGIN OF PARITY)
   MOVWF REG_00 ; 1 ;
READ_PARITY_DELAY ; ;
   DECFSZ REG_00,SAME ; ;FOR ( COUNTER = 0X14;COUNTER != 0X00;COUNTER-- );
   GOTO READ_PARITY_DELAY ;?71;
   MOVLW TRI_B_MASK & 0FEH ; 1 ; RB.0 = OUTPUT ( ACTIVE LOW )
   BSF STATUS,RP0 ; 1 ; PAGE SELECT
   MOVWF TRISB ; 1 ; SET DATA DIRECTION
   BCF STATUS,RP0 ; 1 ; PAGE SELECT
   MOVLW 014H ; 1 ;---> PARITY_ERROR !!!!!!!!!!!!
   MOVWF REG_00 ; 1 ;
READ_STOPBIT_DELAY1 ; ;
   DECFSZ REG_00,SAME ; ;FOR ( COUNTER = 0X1F;COUNTER != 0X00;COUNTER-- );
   GOTO READ_STOPBIT_DELAY1 ;?59;
   MOVLW TRI_B_MASK & 0FFH ; 1 ; RB.0 = INPUT ( TRISTATE )
   BSF STATUS,RP0 ; 1 ; PAGE SELECT
   MOVWF TRISB ; 1 ; SET DATA DIRECTION
   BCF STATUS,RP0 ; 1 ; PAGE SELECT
   DECFSZ REG_02 ;1/2;---> ISORXD IDLE
   GOTO RECEIVE_BYTE ; 2 ;
READ_ERROR ; ;
   BCF STATUS,C ; 1 ;
   RETLW 0 ; 2 ;
; END OF _RECEIVE_ISO_ASYNC

    PAGE
```

```
;*******************************************************************************
;* MODULE :
;* USING :
;* INPUT PARAMETERS :
;* OUTPUT PARAMETERS :
;* DESCRIPTION :
;*******************************************************************************
WREE_C_MODE
   BCF INTCON,GIE ; 1 ; CLOSE ALL INTERRUPTS
   MOVLW C_MODE_EE_ADR ; 1 ;
   MOVWF EEADR ; 1 ; PREPARE ADDRESS
   MOVF C_MODE,WREG ; 1 ;
   MOVWF EEDATA ; 1 ; PREPARE DATA
   BSF STATUS,RP0 ; 1 ;PAGE 1 +++++
   BSF EECON1,EE_WREN ; 1 ; ENABLE WRITE
EEWRITE ; ;
   MOVLW 055H ; 1 ; WRITE SEQUENCE
   MOVWF EECON2 ; 1 ;
   MOVLW 0AAH ; 1 ;
   MOVWF EECON2 ; 1 ;
   BSF EECON1,EE_WR ; 1 ; SET WR BIT
WAIT_EE ; ; BEGIN WRITE
   BTFSC EECON1,EE_WR ; 1 ;
   GOTO WAIT_EE ; 2 ; WAIT FOR WRITE COMPLETE
   BCF EECON1,EE_EEIF ; 1 ; CLEAR EEIF FLAG
   BCF EECON1,EE_WREN ; 1 ; DISABLE WRITE
   BCF STATUS,RP0 ; 1 ;PAGE 0 +++++
   RETURN ; 1 ;

; ORG 2000H ; ; ID 1...4
; DATA 000H ; ;
; DATA 000H ; ;
; DATA 001H ; ;
; ORG 2007H ; ; CONFIGURATION WORD
; DATA 011H ; ; XT OSZ.; WD OFF; PWRTE OFF;
; ; CP ON
END
```

PIC84.H

```
LIST L=ON

;NAME.....VALUE.....TYPE

;-----------------------------------------------------
   PIC84   EQU 000H  ;RESET VECTOR
   RTCC   EQU 1H  ;
   PC   EQU 2H  ;
   STATUS   EQU 3H ;F3 REG IS STATUS REG.
   ; STATUS REG. BITS
   C   EQU 0H  ; CARRY
   DC   EQU 1H  ; DIGITAL CARRY
   Z   EQU 2H  ; ZERO
   PD   EQU 3H  ; POWER DOWN
   TO   EQU 4H  ; T_OUT
   RP0   EQU 5H ;STATUS BITS
   RP1   EQU 6H ;STATUS BITS
   IRP   EQU 7H ;STATUS BITS
   INTCON   EQU 00BH  ;INTCON REGISTER
   GIE   EQU 7H ;INTCON REGISTER BITS
   EEIE   EQU 6H ;INTCON REGISTER BITS
   RTIE   EQU 5H ;INTCON REGISTER BITS
   INTE   EQU 4H ;INTCON REGISTER BITS
   RBIE   EQU 3H ;INTCON REGISTER BITS
   RTIF   EQU 2H ;INTCON REGISTER BITS
   INTF   EQU 1H ;INTCON REGISTER BITS
   RBIF   EQU 0H ;INTCON REGISTER BITS
   EEDATA   EQU 008H  ;16C84 EEPROM DATA REG.
   EEADR   EQU 009H  ;16C84 EEPROM DATA REG.
   EECON1   EQU 088H  ;16C84 EEPROM CONTROL REG. 1
   EE_RD  EQU 000H  ;16C84 READ CONTROL BIT
   EE_WR  EQU 001H  ;16C84 WRITE CONTROL BIT
   EE_WREN  EQU 002H  ;16C84 WRITE ENABLE BIT
   EE_WRERR EQU 003H  ;16C84 WRITE ERROR BIT
   EE_EEIF  EQU 004H  ;16C84 WRITE COMPLETE BIT
   EECON2   EQU 089H  ;16C84 EEPROM CONTROL REG. 2
   FSR   EQU 4H  ;
   PORT_A   EQU 5H
   PORT_B   EQU 6H ; I/O PORT ASSIGNMENTS
   LATCH_A_MASK  EQU B'00000100' ; RA.2 = INPUT
   LATCH_B_MASK  EQU B'00001001' ; RB.0 = I/O, RB.3 = INPUT
   TRISA   EQU 85H ;SPECIAL-PURPOSE REGISTERS
   TRISB   EQU 86H ;SPECIAL-PURPOSE REGISTERS
   TRI_A_MASK  EQU B'00000100' ; RA.2 = INPUT
   TRI_B_MASK  EQU B'00001001' ; RB.0 = I/O, RB.3 = INPUT
   SOLDPO1   EQU PORT_A  ;SOLDER 1 PORT
   SOLDPI1   EQU 2H  ;SOLDER 1 INPUT_PIN RA.2
   SOLDPO2   EQU PORT_B  ;SOLDER 2 PORT
   SOLDPI2   EQU 3H  ;SOLDER 2 INPUT_PIN RB.3

;-----------------------------------------------------
   IND0   EQU 000H  ; FILE
```

```
COM_PORT  EQU PORT_B  ; FILE
ISORXD  EQU 000H  ; BIT
ISOTXD  EQU 000H  ; BIT
FLAGS   EQU 00CH  ; FILE
CONVENTION EQU 000H  ; BIT
CHCKSUM_REQUEST EQU 001H  ; BIT
DECODE_ON_WRITE EQU 002H  ; BIT
DECODE_ON_READ EQU 003H  ; BIT
SEND_REG_B1 EQU 004H  ; BIT
INC_REQUEST EQU 005H  ; BIT
STRING_REQUEST EQU 006H  ; BIT
CHECKSUM_OK EQU 007H  ; BIT
REG_00   EQU 00DH  ; FILE
REG_01   EQU 00EH  ; FILE
REG_02   EQU 00FH  ; FILE
REG_03   EQU 010H  ; FILE
SEND_BYTE  EQU REG_03  ; FILE
READ_BYTE  EQU REG_03  ; FILE
REG_04   EQU 011H  ; FILE
PSW   EQU REG_04  ; FILE
PARITY  EQU 000H  ; BIT
REG_05   EQU 012H  ; FILE
INSTRUCTION_CLASS EQU 013H  ; FILE
INSTRUCTION_CODE EQU 014H  ; FILE
DUMMY1   EQU 015H  ; FILE
COUNTER   EQU 016H  ; FILE
CHECKSUM  EQU 017H  ; FILE
DEC_KEY_POINTER  EQU 018H  ; FILE
REG_B1_POINTER  EQU 019H  ; FILE
REG_47   EQU 01AH  ; FILE
ARRAY_REG_B1  EQU 01BH  ; FILE ( 1B....22 )
FLAGS1   EQU 023H  ; FILE
STR_HEADER EQU 000H  ; BIT
DATA_HEAD EQU 001H  ; BIT
READ_82  EQU 002H  ; BIT
A82_HEADER EQU 003H  ; BIT
WORK   EQU 024H  ; FILE
OSD_COUNT  EQU 025H  ; FILE
C_MODE   EQU 026H  ; FILE
C_MODE_EE_ADR  EQU 000H  ; EEPROM ADDRESS C_MODE
;
SAME   EQU 1H
WREG   EQU 0H
;
LSB   EQU 0H
MSB   EQU 7H
;
TRUE   EQU 1H
YES   EQU 1H
FALSE   EQU 0H
NO   EQU 0H
;
```

16C84 Object Listing Of Ho Lee Fook Hack

```
:020000000029D5
:1000080090082073F34FA34113425340034004AF
:100018000134B034023400340034D3459340034DF
:1000280081348034820700347034783478347C34F4
:100038007E34823472347434763480340030250240
:10004800031D2B28231C2928003423148034193030
:100058001607820 7D83447344F344C344434433479
:1000680041345234443420343134 2E34343443341B
:1000780052345934503454344D344F344434453464
:100088003A3430340F30A6052608303E080082077F
:100098006534E73471341A34B4348834D734763458
:1000A8002834D0344C346E3486348C34C8344334D9
:1000B800A934EC34603442340534F2343D341C3411
:1000C8006C34BC34AF34C3342B34B534DC349034A2
:1000D800F9340534EA34513446349D34E23460341A
:1000E80070345234673426346134493442340934 24
:1000F800503499349034A23436340E34FD343934C3
:100200007F30620000308300043083168500831243
:10021000043085000930831686008312093086007 9
:100220000C108C130C11A301A4010630A5000030A2
:1002300089008316081483120808A600C0218C10B8
:100240008C110C120C1323102311A31113308400F2
:10025000882203 1C1F29882288228403882288225E
:1002600053301302031936296E30BC290A308D0031
:100270000D08162014020319412 98D0B38296D3001
:10028000BC2907300D02031C9B2976301402031D84
:1002900053290630A5000F30A60AA6050930260 20C
:1002A0000318A601E52274301402031D5B290030F7
:1002B0002502031DA50B74301402031D63298C1540
:1002C0000C158C148C131408402297011330840 0F1
:1002D000882210089400 8C1D932906301602031CF6
:1002E000862988229603882296038C161E301602D1
:1002F0000319C8211B3016020319E2211830160217
:100300000319EE2103300E229A0193291A08930053
:1003100014089A001603031993298C1202300E2236
:10032000990A07309905960B66298C1CBB299708FA
:1003300003198C17BB291408402278301402031DBE
:10034000A8290C161A08930040300C1910220C1121
:100350007A30140203190C179609960A00010C1B37
:1003600022208C1B0C1EB829233016078400000 89D
```

```
:10037000402296OFAE29903040220030402 21F29A3
:10038000920112080520402292OA121EC12900344F
:1003900099019801A310131AA314E8301302EF393E
:1003A000031D8C11031D0C11052233301402000 1B2
:1003B000031808309800 3B30140218080318183 04E
:1003C00098000034A318ED2914081504031DED2925
:1003D000052201309B008C110C110034093083166A
:1003E000860083120930860086 19FD290F30130517
:1003F000A40007302405031901 2A260E130503194A
:10040000042A05228C110C1100349B019C019D01D2
:100410009E019F01A001A101A20100348C1D0034A6
:10042000900013308F000F08840000088D001B30EF
:10043000190784009 90A073099050D088006000EF7
:100440000F3918074B208E0000080F391038180795
:100450004B208E078E090E088E0703188E0A0D0892
:100460008E070E088E0703188E0A8E0E1B30190792
:10047000840 00E0880068C1A8F0A900B132A003411
:10048000061090000F308F0006308E001E308D0059
:100490008D0B482A8E0B462A09308E0091010C1CC8
:1004A00090090C1C910A0310592A0C18900C0C1C72
:1004B000900D0318910A0930031C0830831686003A
:1004C000831219308D008D0B632A000000008E0B03
:1004D000552A02308D008D0B6B2A0930111C083013
:1004E000831686 0083121D308D008D0B752A000047
:1004F000093083168600831219308D008D0B7E2AF9
:10050000061862A8F0B442A031000340314003483
:1005100006100F308F0032308E008D01061C061839
:10052000922A972A8D0B8E2A8E0B852AE32A083068
:100530008E008001910129308D008D0B9D2A8D0147
:100540000C1C8D1406188D0A06188D0A06188D0AC3
:100550008D18910A03108D1803140C18800C0C1CB4
:10056000800D17308D008D0BB32A000000008E0B1C
:100570009F2A8D010C1C8D14000006188D0A061888
:100580008D0A06188D0A111C8D098D1CD12A383050
:100590008D008D0BC92A000890009707840A031468
:1005A000003418308D008D0BD32A08308316860056
:1005B000831214308D008D0BDB2A093083168600E0
:1005C00083128F0B8B2A031000348B1300308900A9
:1005D000260888008316081555308900AA3089003E
:0E05E00088148818F12A0812081183120800E6
:00000001FF
```

The OMIGOD Hack

Well after the Ho Lee fook, the OmiGod was the logical progression. The OmiGod, (pronounced Oh My God), was a PC Emulator for VideoCrypt. The program is public domain software. The name of the hack is SEASON7. The SEASON7 intended to be a reference to the seventh season of Star Trek - The Next Generation. Many hackers have referred to the hack as the OMIGOD hack.

When an IBM compatible personal computer is connected to a VideoCrypt decoder, the program will ran on the computer and will emulated a valid Sky 07 issue smart card. The effect of this hack on the market has yet to be established but it definitely caused problems for Sky and News Datacom. It was the ultimate insult for News Datacom - computer hobbyists were able to run the hacks on their home computers. There were versions for the BBC Archimedes and the Apple Mac computers as well.

The program was created for use outside of the UK. The reason for its creation is Star Trek. Apparently Sky has refused to provide subscriptions outside of its own copyright area. The direct result of this has been to irritate those who would honestly subscribe, if they were allowed to.

When the program was released it spread like wildfire. The method of release was similar to that of shareware. The Usenet and the bulletin boards ensured that it covered Europe in a matter of a few hours. Though its use in the UK will be illegal, there was no possible way to stop its distribution in the UK. Sky and News Datacom could not close down every international telephone line and neither can they close down every UK BBS.

There were some rumours that the program would be released via the Delphi system in the USA. This internet system apparently was bought by Rupert Murdoch some time ago. If this occurred it would be an elegant hack.

The interface is a very simple circuit consisting of a MAX232 and a 74LS07. The MAX232 converts the levels between RS232 and TTL and the 74LS07 is an open collector buffer. The MAX232 generates the two positive and negative RS232 voltages internally. This means that the card power supply line from the decoder can drive the interface directly.

The interface can be constructed on a printed circuit board or a piece of stripboard. The main disadvantage for some people will be the connection of the interface to the decoder. The most logical method would be via the card socket. The problem is that a dummy smart card would have to be etched.

The standard fibreglass printed circuit board material is 1.6 millimetres thick. The thickness of the smart card is roughly half of this. Where PCB material of the correct thickness was not available, it was common to sand down a 1.6 mm piece of PCB. The etching would be carried out first. The resultant PCB would be longer than the official smart card. Some people have suggested using the defunct pirate cards instead.

The direct connection of the interface to the decoder is also possible. The only connections to the decoder are the data line, the 5 Volt Vcc line, Ground and RESET. This is of course a risky option for those unfamiliar with the circuitry. Full details of the interface are given in the Smart Card section at the back of the book.

Delayed Data Transfer

The DDT hack is currently the most reliable hack on the VideoCrypt system. Indeed it should work on any implementation of the VideoCrypt across the planet. The only potential flaw would be if the VideoCrypt implementation under attack used the Fiat Shamir ZKT.

The letters DDT stand for Delayed Data Transfer or Transmission. However the effect on VideoCrypt would be similar to the pesticide of the same name.

The flaw that allows this hack to work is that the data rate of the control packets on the VideoCrypt system is approximately 1 kilobaud. This data rate is slow enough to allow the signal to be recorded on a standard video tape recorder. Of course there are some VCRs that do not record the VBI lines that carry the data.

The principle of the hack is that the key stream from a valid card can be recorded and stored. This keystream can then be played back to a decoder that is being fed with a scrambled recording of the programme that the keystream was made for. The decoder will decode the scrambled signal as the keystream is played back as if it was a that from a valid smart card.

The keystreams for various programmes have already been posted on various BBSes and FTP sites. Mainly these streams have been for "The Simpsons", "Star Trek:TNG", "The X-Files" and "Deep Space 9". No doubt the keystream for the movie "Sneakers" will also be posted.

Some people have commented that this hack is not really a true hack. I would disagree with this. It is a very elegant hack and, most importantly, it works.

Perhaps the effective use of this hack will be in the area of Pay Per View. Normally when PPV is considered, the programming is thought of in terms of such as concerts or sporting events. While these do form part of a PPV channel, the real attraction is in first run movies. This is exactly the type of programming at which the hack excels.

The runtime versions of both of these hacks are available on a number of BBSes and FTP sites in Europe including Special Projects BBS (+353-51-50143).

Official Specification For The VCL File Format

The essential data for decoding the scrambled VideoCrypt signal is the 74h/78h pair. These are the message block and the key packets respectively . Much of the rest of the data traffic is card authorisation and deauthorisation data.

The VCL format uses this redundancy to save storage space. Only 12 bytes of high entropy (that means: almost uncompressable) are stored every 2.5 seconds. Therefore a VCL file of a 1 hour programme is only about 17 kilobytes large. In addition, VCL files do not contain information about the card owner (especially the card serial number), which appears in normal full log files in the 70h and 7Ch packets. (The only potential security hole is the remaining nibble in the 78h key packet. Consequently it should be cleared in order to avoid card specific information to leak into the VCL file.)

VCL files have a very simple binary format consisting of a 128 byte header and a specified number of 12 byte records. At the end, VCL files may be padded with zero bytes to a multiple of the operating system's disk sector size, so that no RAM contents can leak into the file out of an insecure system like MS-DOS. Don't forget to use a binary mode if you transfer VCL files or their contents will be rendered unusable.

The 128 Byte VCL File Header Format

Bytes 0 - 3

ASCII String 'VCL1' which identifies the file type and version of the format.

Bytes 4 - 7

The number of 12-byte records stored in this file encoded as a bigendian (most significant byte first) 32-bit unsigned integer value.

Bytes 8 - 23

Date and time when the recording started. Format: yyyymmddThhmmssZ, where yyyymmdd are year, month and day (e.g. '19940618'), hhmmss are hour, minute and second (e.g. '235959'), T is just the ASCII letter T, and Z is the ASCII letter Z if the time is UT C or a zero byte, if the time is local time. The digits are ASCII characters.

Bytes 24 - 55

Name of the satellite or cable system from which the recording was done. This is a zero terminated ASCII string with only characters between 20h and 7Eh. As many zero bytes are appended as necessary for filling up the 32 bytes. The same format is also used for the next two text fields. Example: 'Astra'.

Bytes 56 - 63

Name/number of the transponder from which the recording was done. Example: '08' for Sky One on Astra.

Bytes 64 -127

Description of what has been recorded. Example: 'Star Trek: TNG, episode 123'

The first 128 bytes are followed by as many 12 byte records that are specified in bytes 4-7. Each record represents a 74h/78h Videocrypt protocol pair and consists of two fields: The first 4 bytes are the final 4 bytes of the 74h message packet part, the remaining 8 bytes are the data part of the corresponding 78h key packet. Four bytes of each 74h packet are enough to allow a card emulator to quickly and reliably synchronize with the queries of the decoder. The final four bytes of the 74h commands have been selected because of their high entropy (signature and checksum).

DECRYPT.H

```
/* prototypes for decrypt.c */
  int decode(const unsigned char *msg, unsigned char *answ)
```

ASYNC.H

```
  #ifndef _ASYNC_H_
  #define _ASYNC_H_
  int AsyncInit( int Port);
  void AsyncStop( void),
   AsyncClear( void),
   AsyncOut( int c),
   AsyncHand( int handshake),
   AsyncSet( int Baud, int Control);
  int AsyncIn( void),
   AsyncInStat( void),
   AsyncOutStat( void);
  unsigned AsyncStat( void);
  #define COM1 0
  #define COM2 1
  #define COM3 2
  #define COM4 3
/* Defines for Com Port Paramaters, the second paramater to AsyncSet() */
  #define BITS_8 0x03
  #define BITS_7 0x02
  #define STOP_1 0x00
  #define STOP_2 0x04
  #define EVEN_PARITY 0x18
  #define ODD_PARITY 0x08
  #define NO_PARITY 0x00
/* Defines for AsyncHand() */
  #define DTR 0x01
  #define RTS 0x02
  #define USER 0x04
  #define LOOPBACK 0x10
/* Defines for AsyncStat() */
  #define D_CTS 0x0100
  #define D_DSR 0x0200
  #define D_RI 0x0400
  #define D_DCD 0x0800
  #define CTS 0x1000
  #define DSR 0x2000
  #define RI 0x4000
  #define DCD 0x8000
  #define PARITY 0x0004
  #define THREMPTY 0x0020
```

```
#define BREAKDET 0x1000
#endif
```

DECRYPT.C

```
/*
* This module contains the critical algorithm and secret key
* used by British Sky Broadcasting in their Videocrypt pay-TV
* chip card in 1993 and early 1994. It is expected that most
* information in this file becomes obsolete when the next card
* generation (09) is activated.
 */
#define WITH_ADULT
#include ''decrypt.h''
/*
* the secret keys -- for your eyes only :-)
*/
const unsigned char sky_keys[56] = {
0x65, 0xe7, 0x71, 0x1a, 0xb4, 0x88, 0xd7, 0x76,
0x28, 0xd0, 0x4c, 0x6e, 0x86, 0x8c, 0xc8, 0x43,
0xa9, 0xec, 0x60, 0x42, 0x05, 0xf2, 0x3d, 0x1c,
0x6c, 0xbc, 0xaf, 0xc3, 0x2b, 0xb5, 0xdc, 0x90,
0xf9, 0x05, 0xea, 0x51, 0x46, 0x9d, 0xe2, 0x60,
0x70, 0x52, 0x67, 0x26, 0x61, 0x49, 0x42, 0x09,
0x50, 0x99, 0x90, 0xa2, 0x36, 0x0e, 0xfd, 0x39
};
#ifdef WITH_ADULT
const unsigned char adult_keys[96] = {
```

Note: This key table is provided on a page at the back of the book. This is due to distribution conditions in the UK where the key table may have to be omitted. However the keytable is widely available on BBSes all over Europe and therefore is more or less in the public domain anyway.

```
};
#endif
```

```
/*
* This is the core function of the secure hash algorithm
* which is called 99 times by hash(). This code assumes that
* unsigned char is exactly 8-bit long.
*/
  void kernel(unsigned char *out, int *oi, const unsigned
  char in,
  const unsigned char *key)
  {
  unsigned char c;
  out[*oi] ^= in;
  c = ~(key[out[*oi] >> 4] + key[(out[*oi] & 0x0f) + 16]);
  c = (c << 1) | (c >> 7); /* rotate 1 bit left */
  c += in;
  c = (c >> 3) | (c << 5); /* rotate 3 bit right */
  *oi = (*oi + 1) & 7;
  out[*oi] ^= c;
  return;
  }
/*
* This is a secure hash function that transforms a 32-byte message
* in an 8-byte answer sequence and tests a 4-byte signature and a 1-byte
* checksum in the 32-byte message. The transformation and the signature
* check are done using a secret 32-byte key. This function is designed
* in a way that makes it very difficult to guess the key bytes or to
* write an identical function without knowing the key bytes by
* looking only at the results of this function.
*/
  int hash(const unsigned char *msg, unsigned char *answ,
  const unsigned char *key)
  {
  int i;
  int oi = 0; /* index in output array answ[] */
  int check = 0; /* flag for incorrect signature/checksum */
  unsigned char b = 0;
  for (i = 0; i < 8; i++) answ[i] = 0;
/* initial hashing */
  for (i = 0; i < 27; i++)
  kernel(answ, &oi, msg[i], key);
/* check the 4 signature bytes and continue hashing */
  for (i = 27; i < 31; i++) {
  kernel(answ, &oi, b, key);
  kernel(answ, &oi, b, key);
```

```
  b = msg[i];
  if (answ[oi] != msg[i]) check |= 1; /* test signature */
  oi = (oi + 1) & 7;
  }
/* final hashing with last byte */
  for (i = 0; i < 64; i++)
  kernel(answ, &oi, msg[31], key);
  /* test 8-bit checksum */
  b = 0;
  for (i = 0; i < 32; i++)
  b += msg[i];
  if (b != 0) check |= 2;
  answ[7] &= 0x0f; /* only 60-bit are needed by decoder */
  return check;
  }
/*
* The decoder requests every ~2.5 seconds an answer to a 32-byte
* packet (msg) from the chip card. The card's 8-byte answer (answ) to
* this request is calculated by this function using hash() and the
* right key bytes.
*/
  int decode(const unsigned char *msg, unsigned char *answ)
  {
  int i;
  int check; /* flag for incorrect signature/checksum */
  const unsigned char *key; /* pointer to the 32-byte key to
  be used */
/* select Sky key */
  if (msg[1] > 0x3a) key = sky_keys + 24;
  else if (msg[1] > 0x32) key = sky_keys + 8;
  else key = sky_keys;
  check = hash(msg, answ, key);
/* following 0xa0 fix has been necessary since 1994-04-27 */
  if ((msg[6] & 0xf0) == 0xa0)
  for (i = 0; i < 8; i++) answ[i] = 0;
  if ((check & 1) == 0) return check | (1 << 2);
/* Sky key was ok */
  #ifdef WITH_ADULT
/* if Sky failed, try Adult Channel */
  if (msg[1] > 0x4a) key = adult_keys + 48;
  else if (msg[1] > 0x43) key = adult_keys + 40;
  else if (msg[1] > 0x3a) key = adult_keys + 32;
  else if (msg[1] > 0x33) key = adult_keys + 8;
  else key = adult_keys;
  check = hash(msg, answ, key);
  if ((check & 1) == 0) return check | (2 << 2);
```

```
/* Adult key was ok */
  #endif
/* no known key resulted in a correct signature test */
  for (i = 0; i < 8; i++) answ[i] = 0;
  return check;
  }
```

SEASON7.C

```
/*
* Season7 -- Videocrypt smart card emulator for DOS.
*
* Compiles e.g. with Borland C++ 2.0, small model.
*/
  #include <stdio.h>
  #include <stdlib.h>
  #include <ctype.h>
  #include <string.h>
  #include <time.h>
  #include <conio.h> /* for kbhit() & clrscr() */
  #include <dos.h> /* for int86() */
  #include ''decrypt.h''
  #include ''async.h''
  #define VERSION ''1.3''
/* last change: 1994-06-18 */
/*
* information in answer to reset: (as defined in ISO 7816-3)
* inverse convention (3f), protocol type T=0, F=372, D=1, I=50mA, P=5V,
N=5.
* historic characters (final 10 bytes): ???
*/
  int reset_answer_len = 16;
  char reset_answer[33] = {
  0x3f, 0xfa, 0x11, 0x25, 0x05, 0x00, 0x01, 0xb0,
  0x02, 0x3b, 0x36, 0x4d, 0x59, 0x02, 0x81, 0x80
  };
/* we show this shortly after a reset on the screen */
  unsigned char display[25] =''\x80''
  ''SEASON7 V'' VERSION
  '' --:-- '';
/* BSkyB channel id (based on byte 7 in 74 messages) for TV screen display
```

```
*/
  char *channel_id[16] = {
  '' ???? '', '' SKY MOVIES '', ''MOVIECHANNEL'', ''MOVIES
  GOLD'',
  '' ???? '', '' ???? '', '' SKY SPORTS '', '' ???? '',
  '' TV ASIA '', '' ???? '', '' ???? '', '' ???? '',
  ''MULTICHANNEL'', '' ???? '', '' ???? '', '' ???? ''
  };
/* BSkyB channel name for text screen display */
  char *channel_name[16] = {
  ''???'', ''Sky Movies'', ''The Moviechannel'', ''Sky
  Movies Gold'',
  ''???'', ''???'', ''Sky Sports'', ''???'',
  ''TV Asia'', ''???'', ''???'', ''???'',
  ''Sky Multichannels'', ''???'', ''???'', ''???''
  };
/* message directions */
  #define IN 0 /* to card */
  #define OUT 1 /* to decoder */
/*
* These are some delay values (microseconds) used in the program.
* Use command line option w to modify them.
*/
  #define DELAYS 2
  unsigned long delus[DELAYS] = {
  30000, /* wait between reset and answer to reset */
  500, /* wait after each outgoing byte */
  };
/*
* Reverse and invert all bits in each byte of a string.
* E.g. 10010111b (0x97) becomes 00010110b (0x16).
*/
  void inverse(char *data, int len) {
  int i, j;
  unsigned char c;
  for (i = 0; i < len; i++) {
  c = 0;
  for (j = 0; j < 8; j++)
  c |= ((data[i] & (1 << j)) != 0) << (7 - j);
  data[i] = ~c;
  }
  return;
  }
```

```
/*
* Uses a BIOS function in order to wait a specified number of
* microseconds. This BIOS functions is only implemented in
* IBM AT compatible BIOSes (i.e., not in old PC and XT systems)!
* The timing resolution of this function isn't really down
* to 1 us on most systems, but it's fine for our purposes.
*/
  void wait_us(unsigned long microseconds)
  {
  union REGS regs;
  if (microseconds == 0) return;
  regs.h.ah = 0x86;
  regs.x.cx = (int) (microseconds >> 16);
  regs.x.dx = (int) (microseconds & 0xffff);
  int86(0x15, &regs, &regs);
  return;
  }
  void activate_com(int com)
  {
  int port;
  switch (com) {
  case 1: port = COM1; break;
  case 2: port = COM2; break;
  case 3: port = COM3; break;
  case 4: port = COM4; break;
  default:
  printf(''Port COM%d not available!\n'', com);
  exit(1);
  }
  if (AsyncInit(port)) {
  printf(''Can't initialize port COM%d!\n'', com);
  exit(1);
  }
  AsyncHand(DTR | RTS);
  AsyncSet(9600, BITS_8 | STOP_2 | ODD_PARITY);
  return;
  }
  void deactivate_com(void)
  {
  AsyncStop();
  }
```

```
/*
* Send a string of bytes to serial port and wait for each single echo.
* (More efficient send methods are too fast for decoder, it seems to
* need more than 2 stop bits, so we wait between individual bytes.)
*/
  int send(char *data, int len)
  {
  int i;
  char c;
  AsyncClear();
  for (i = 0; i < len; i++) {
  c = data[i];
  inverse(&c, 1);
  AsyncOut(c);
  while (AsyncInStat() == 0)
  if ((AsyncStat() & DCD) || kbhit()) return 1;
  AsyncIn();
  wait_us(delus[1]);
  }
  return 0;
  }
/*
* Get all bytes available from serial port FIFO and return how many
* bytes were available.
*/
  int receive(char *data, int max)
  {
  int i = 0;
  while (AsyncInStat() > 0 && i < max)
  data[i++] = AsyncIn();
  inverse(data, i);
  return i;
  }
/*
* Get n bytes from serial port FIFO. Don't wait more than timeout
* microseconds and return how many bytes were available.
*/
  int receive_timeout(char *data, int n, long timeout)
  {
  int i = 0;
  while (i < n && timeout > 0)
  if (AsyncInStat() > 0)
  data[i++] = AsyncIn();
  else {
  wait_us(15000);
  timeout -= 15000;
```

```
  }
  inverse(data, i);
  return i;
  }
/*
* In debugging mode, print the contents of all packets.
*/
  void log_packet(unsigned char *header, unsigned char
  *data,
  int direction)
  {
  int i, j;
  static time_t last_time = 0;
  time_t now;
  char tmp[40];
  /* print time from time to time */
  time(&now);
  if (difftime(now, last_time) >= 10) {
  strftime(tmp, 40, ''%Y-%m-%d %H:%M:%SZ'', gmtime(&now));
  printf(''%s\n'', tmp);
  last_time = now;
  }
  if (header[1] == 0x60) /* illegal command code 0x60: reset
  */
  printf(''RESET: '');
  else
  printf(''%s %02x: '', (direction == IN) ? ''dcdr'' :
  ''card'', header[1]);
  for (i = 0; i < header[4]; i += 16) {
  if (i > 0) printf('' '');
  for (j = 0; j < 16; j++)
  if (i + j < header[4])
  printf(''%02x '', data[i + j]);
  else
  printf('' '');
  printf('' '');
  for (j = 0; j < 16 && i + j < header[4]; j++)
  putchar((data[i + j] > 31 && data[i + j] < 127) ? data[i + j]
  : '.');
  putchar('\n');
  }
  return;
  }
```

```
/*
* Parse an answer to reset packet.
*
* Return value: >0 correct answer to reset received, length returned
* -1 no correct answer to reset received
*/
  int parse_reset(void)
  {
  int y, p, i, tck_expected = 0;
  reset_answer_len = 0;
/* Skip reset impulse noise characters and read TS */
  reset_answer[0] = 0;
  for (i = 0; i < 5 && reset_answer[0] != 0x3f; i++)
  if (receive_timeout(reset_answer, 1, 500000L) == 0) return
  -1;
  if (reset_answer[0] != 0x3f) return -1;
/* Read T0 */
  if (receive_timeout(reset_answer + 1, 1, 500000L) == 0)
  return -1;
/* Read TA_i, TB_i, TC_i, TD_i */
  p = 2;
  y = reset_answer[1] >> 4;
  while (y && p < 33 - 5 - (reset_answer[1] & 15)) {
  for (i = 0; i < 4; i++) {
  if ((y >> i) & 1) {
  if (receive_timeout(reset_answer + p, 1, 500000L) != 1)
  return -1;
  if (i == 3) {
  tck_expected |= (reset_answer[p] & 15) != 0;
  y = reset_answer[p] >> 4;
  }
  p++;
  } else
  if (i == 3) y = 0;
  }
  }
/* while () */
/* historic characters */
  if (receive_timeout(reset_answer + p, reset_answer[1] &
  15, 500000L) !=
  (reset_answer[1] & 15))
  return -1;
  p += (reset_answer[1] & 15);
/* TCK */
  if (tck_expected) {
```

```
  if (receive_timeout(reset_answer + p, 1, 500000L) != 1)
  return -1;
  p++;
  y = 0;
  for (i = 1; i < p; i++)
  y ^= reset_answer[i];
  if (y != 0) return -1;
  }
/* everything was fine */
  reset_answer_len = p;
  return p;
  }
  main(int argc, char **argv)
  {
  unsigned char header[5];
  int hc = 0, received = -1, length, dir;
  unsigned char buffer[65];
  unsigned char msg[32];
  unsigned char seed[8];
  unsigned char *data;
  char proc_byte;
/* procedure byte in passive mode */
  int sw2_next = 0;
/* second procedure byte SW2 will follow */
  int sw2_ok = 0;
/* second procedure byte SW2 has been received */
  int sync_lost = 1;
  time_t now;
  char *current_name = ''???'';
  int station = 0;
  int com = 2;
  int debug = 0, quit = 0, message = 1;
  int economy = 0;
  int passive = 0;
/* passive==1: Season7 listens only to card traffic */
  int suspended = 0;
  int i, j, k, c;
  #define LOGMAX 400
  time_t logtime[LOGMAX], start;
  unsigned char logmsg[LOGMAX][32];
  int loglength = 0, lognext = 0, check;
  char *logfn = ''VCLOG'';
  char satellite[80], transponder[80], program[80];
  char tmp[129], fn[16];
  FILE *f;
  FILE *vcl_out = NULL, *vcl_in = NULL;
  char *vcl_out_fn = NULL, *vcl_in_fn = NULL;
  unsigned long vcl_count = 0, l;
```

```
  unsigned vcl_current = 0, u;
  long *vcl_msg_hash;
  char (*vcl_seed)[8];
  #ifndef __MSC
  clrscr();
  #endif
  fprintf(stderr, ''\nSeason7 -- Version '' VERSION
  '' -- Videocrypt smart card emulator\n\n'');
  fprintf(stderr,
  ''Important: This software must not be used in order to view
  channels\n''
  '' for which a regular subscription would be available
  in\n''
  '' your country, unless you have already such a subscrip-
  tion\n''
  '' and want to use this software only for educational\n''
  '' purposes.\n\n'');
  tzset(); /* get local time zone from environment variable
  TZ */
  time(&start);
  for (i = 1; i < argc; i++) {
  if (isdigit(argv[i][0]))
  com = atoi(argv[i]);
  else
  for (j = 0; j < 999 && argv[i][j]; j++)
  switch(argv[i][j]) {
  case 'd':
  case 'D':
/* switch on screen log mode */
  debug = 1;
  break;
  case 'p':
  case 'P':
/* activate passive mode: Season7 is now only listening */
  passive = 1;
  break;
  case 'm':
  case 'M':
/* suppress TV display messages */
  message = 0;
  break;
  case 'e':
  case 'E':
/* economy mode: avoid time consuming tasks like printf()s
* in order to allow stable operation on very slow systems */
  economy = 1;
  break;
  case 'o':
  case 'O':
```

```
/* produce a VCL (videocrypt card log) file from the data
* recorded in passive mode. */
  if (vcl_out_fn || vcl_in_fn) break;
  fprintf(stderr, ''Which satellite do you receive (Astra):
  '');
  gets(satellite);
  if (strlen(satellite) == 0) strcpy(satellite, ''Astra'');
  fprintf(stderr, ''Which transponder on '%s' do you record
  (08): '',
  satellite);
  gets(transponder);
  if (strlen(transponder) == 0) strcpy(transponder,
  ''08'');
  fprintf(stderr, ''What are you recording: '');
  gets(program);
  fprintf(stderr, ''\n'');
  satellite[31] = 0;
  transponder[7] = 0;
  program[63] = 0;
  for (k = strlen(satellite); k < 32; k++) satellite[k] = 0;
  for (k = strlen(transponder); k < 8; k++) transponder[k] =
  0;
  for (k = strlen(program); k < 64; k++) program[k] = 0;
  if (argv[i][j+1] == '\0') {
  start += 60 * 5; /* round up the hour by 5 minutes */
  strftime(fn, 9, ''vc%m%d%H'', gmtime(&start));
  start -= 60 * 5;
  sprintf(fn + 8, ''.%.1s%.2s'', satellite, transponder);
  vcl_out_fn = fn;
  } else
  vcl_out_fn = argv[i] + j + 1;
  j = 1000;
  passive = 1;
  break;
  case 'i':
  case 'I':
/* read in a VCL file and use it in order to answer the
* hash function queries of the decoder. */
  if (vcl_in_fn || vcl_out_fn) break;
  if (argv[i][j+1] == '\0') {
  fprintf(stderr, ''Specify filename after option i ''
  ''(e.g. 'season7 ivc061817.a08')!\n'');
  exit(1);
  } else
  vcl_in_fn = argv[i] + j + 1;
  j = 1000;
  break;
  case 'w':
  case 'W':
```

```
/*
* modify delay table, e.g. option wb200 waits 200 us after each
* byte because this sets delus['b' - 'a'] = 200.
*/
  k = tolower(argv[i][j+1]) - 'a';
  if (k < 0 || k >= DELAYS || !isdigit(argv[i][j + 2])) {
  printf(''Only wait options between wa<ticks> and ''
  ''w%c<ticks> possible.\n'', 'a' + DELAYS - 1);
  exit(1);
  }
  j += 2;
  delus[k] = atol(argv[i] + j);
  while (isdigit(argv[i][j + 1])) j++;
  break;
  default:
  break;
  }
  }
  fprintf(stderr, ''Press q for exit.\n\n'');
  fprintf(stderr, ''Using serial port COM%d, byte delay %lu
  \xe6s.\n'',
  com, delus[1]);
  strftime(tmp, 80, ''%Y-%m-%d %H:%M:%S'', gmtime(&start));
  fprintf(stderr, ''World time (UTC): %s\n'', tmp);
  if (passive)
  fprintf(stderr, ''Passive mode: only listening to data
  traffic.\n'');
  if (vcl_out_fn) {
  /* open VCL output file */
  vcl_out = fopen(vcl_out_fn, ''wb'');
  if (vcl_out == NULL) {
  fprintf(stderr, ''Sorry, can't open VCL file '%s'',
  vcl_out_fn);
  perror('''');
  exit(1);
  }
  fprintf(stderr, ''Writing VCL file '%s'.\n'',
  vcl_out_fn);
/* Write VCL header (128 bytes) */
  fprintf(vcl_out, ''VCL1'');
/* Magic code, version 1 */
  putc(0, vcl_out);
/* space for number of seeds (bigendian) */
  putc(0, vcl_out);
  putc(0, vcl_out);
  putc(0, vcl_out);
  strftime(tmp, 80, ''%Y%m%dT%H%M%SZ'', gmtime(&start));
  fwrite(tmp, 1, 16, vcl_out);
  fwrite(satellite, 1, 32, vcl_out);
```

```
fwrite(transponder, 1, 8, vcl_out);
fwrite(program, 1, 64, vcl_out);
}
if (vcl_in_fn) {
/* open VCL input file */
vcl_in = fopen(vcl_in_fn, ''rb'');
if (vcl_in == NULL) {
fprintf(stderr, ''Sorry, can't open VCL file '%s'',
vcl_in_fn);
perror('''''');
exit(1);
}
fprintf(stderr, ''Reading VCL file '%s'.\n'', vcl_in_fn);
fread(tmp, 1, 128, vcl_in);
if (feof(vcl_in)) {
fprintf(stderr, ''Unexpected end of VCL input file!\n'');
exit(1);
}
if (strncmp(tmp, ''VCL1'', 4)) {
fprintf(stderr, ''Sorry, '%s' is not a VCL file!\n'',
vcl_in_fn);
exit(1);
}
tmp[55] = tmp[63] = tmp[127] = 0;
printf(''\n%s, transponder %s, %.4s-%.2s-%.2s
%.2s:%.2s:%.2s%.1s\n%s\n\n'',
tmp + 24, tmp + 56, tmp + 8, tmp + 12, tmp + 14,
tmp + 17, tmp + 19, tmp + 21, tmp + 23, tmp + 64);
if (tmp[4] || tmp[5]) {
fprintf(stderr, ''Sorry, VCL file too long for this
implementation.\n'');
exit(1);
}
vcl_count = ((unsigned long)(unsigned char) tmp[6] << 8) |
(unsigned long)(unsigned char) tmp[7];
#if (sizeof(long) != 4)
fprintf(stderr, ''Porting error!\n'');
exit(1);
#endif
vcl_msg_hash = (long *) malloc((size_t) (vcl_count * 4L));
vcl_seed = (char (*)[8]) malloc((size_t) (vcl_count *
8L));
if (!vcl_msg_hash || !vcl_seed) {
fprintf(stderr, ''Not enough memory for %lu bytes (%lu
entries).\n'',
vcl_count * 12, vcl_count);
exit(1);
}
for (l = 0; l < vcl_count; l++)
if (fread(vcl_msg_hash + (unsigned) l, 1, 4, vcl_in) != 4 ||
fread(vcl_seed + (unsigned) l, 1, 8, vcl_in) != 8) {
```

```
  fprintf(stderr, ''Unexpected end of VCL input file!\n'');
  exit(1);
  }
  }
  activate_com(com);
  AsyncStat();
/* clear D_DCD */
  if (economy)
  fprintf(stderr, ''\nOperating ...'');
  else
  fprintf(stderr, ''\nWaiting for reset ...'');
  while (!quit) {
/* keyboard commands */
  if (kbhit()) {
  c = getch();
  switch (c) {
  case 0:
/* ignore function keys */
  getch();
  break;
  case 'q':
  case 'Q':
  case 'x':
  case 'X':
  case 27:
/* abort program */
  quit = 1;
  continue;
  case 'd':
  case 'D':
/* switch on/off screen log */
  debug = !debug;
  printf(''\rDebug mode %s.\t\t\t\t\t\n'', debug ? ''on'' :
  ''off'');
  break;
  case 'l':
  case 'L':
/* write last crypto messages (command 0x74) to a file */
  if (economy) break;
  i = lognext - loglength;
  while (i < 0) i += LOGMAX;
  printf(''\rWriting last %d messages to logfile
  '%s'...\t\t\t\n'',
  loglength, logfn);
  f = fopen(logfn, ''w'');
  if (f == NULL)
  perror(''Sorry, can't open logfile'');
  else {
  strftime(tmp, 80, ''%Y-%m-%d'', gmtime(&logtime[i]));
```

```
  fprintf(f, ''%s\n'', tmp);
  for (j = 0; j < loglength; j++) {
  strftime(tmp, 80, ''%H:%M:%SZ'', gmtime(&logtime[i]));
  fprintf(f, ''%s '', tmp);
  for (k = 0; k < 32; k++)
  fprintf(f, ''%02x'', logmsg[i][k]);
  fprintf(f, ''\n'');
  if (++i >= LOGMAX) i = 0;
  }
  fclose(f);
  }
  break;
  case '+':
/* increase byte delay by 0.5 ms */
  if (delus[1] < 2000) delus[1] += 500;
  printf(''\rByte delay set to %lu \xe6s.\t\t\t\t\t\n'',
  delus[1]);
  break;
  case '-':
/* decrease byte delay by 0.5 ms */
  if (delus[1] >= 500) delus[1] -= 500;
  printf(''\rByte delay set to %lu \xe6s.\t\t\t\t\t\n'',
  delus[1]);
  break;
  case 's':
  case 'S':
  if (!vcl_out || suspended) break;
  printf(''\rVCL file recording suspended.\t\t\t\t\t\n'');
  suspended = 1;
  break;
  case 'c':
  case 'C':
  if (!vcl_out || !suspended) break;
  printf(''\rVCL file recording continues.\t\t\t\t\t\n'');
  suspended = 0;
  break;
  default:
  break;
  }
  }
  if (AsyncStat() & (DCD | D_DCD)) {
/*
* we have a reset and the decoder now expects an
* answer-to-reset packet from the card as described in
* ISO 7816.
*/
  if (!passive || (AsyncStat() & DCD))
```

```
  AsyncClear();
  sync_lost = 0;
  if (!economy) fprintf(stderr, ''\r\t\t\t\t\t\r'');
  if (!economy && !debug)
  printf(''RESET'');
  while ((AsyncStat() & DCD) && !kbhit());
  if (kbhit()) continue;
  if (passive) {
  if (parse_reset() < 0) sync_lost = 1;
  } else {
  wait_us(delus[0]);
  if (send(reset_answer, reset_answer_len)) continue;
  if (!economy && message) {
  now = time(NULL);
  strftime((char *) display + 13, 13, '' %H:%M '',
  localtime(&now));
  display[0] = '\xd8';
  }
  }
  if (debug && !sync_lost) {
  header[1] = 0x60; /* special value indicates log_packet a
  reset */
  header[4] = reset_answer_len;
  log_packet(header, (unsigned char *) reset_answer, 0);
  }
  station = 0;
  hc = 0;
  received = -1;
  sw2_next = 0;
  AsyncStat(); /* clear D_DCD */
  }
  if (passive && sync_lost) {
/*
* In passive mode, we can't just wait for a reset if
* anything went wrong. So we try to resynchronize here
* by waiting for characteristic byte sequences like
* 90 00, 53 7x, or 53 8x. Let's hope this makes the passive mode a
* little bit more robust.
*/
  if (receive((char *) buffer + sync_lost - 1, 1)) {
  if (sync_lost == 1 && (buffer[0] == 0x90 || buffer[0] ==
  0x53)) {
  sync_lost++;
  } else {
  if (sync_lost == 2) {
  if (buffer[0] == 0x90 && buffer[1] == 0x00) {
/* same state as after a reset */
  hc = 0;
```

```
  received = -1;
  sw2_next = 0;
  sync_lost = 0;
  if (!economy) fprintf(stderr, ''\r\t\t\t\t\t\r'');
  } else if (buffer[0] == 0x53 &&
  ((buffer[1] & 0xf0) == 0x70 ||
  (buffer[1] & 0xf0) == 0x80)) {
  header[0] = buffer[0];
  header[1] = buffer[1];
  hc = 2;
  received = -1;
  sw2_next = 0;
  sync_lost = 0;
  if (!economy) fprintf(stderr, ''\r\t\t\t\t\t\r'');
  } else {
/* resynchronization attempt failed, because of 2nd byte */
  sync_lost = 1;
  }
  } /* if (sync_lost == 2) */
  }
  } /* if (receive()) */
  } else if (hc < 5) {
/* waiting for more header bytes */
  hc += receive((char *) header + hc, 5 - hc);
  } else {
  if (received < 0) {
/* new 5 byte command header has arrived */
  if (header[0] != 0x53) {
  if (!passive) {
  send(''\x6e\x00'', 2); /* unsupported class */
  hc = 0;
  } else sync_lost = 1;
  printf(''\rUnsupported class code %02x!\t\t\n'', hea-
  der[0]);
  } else {
  data = buffer;
  memset(buffer, 0, 64); /* default answer: 00 00 00 ... */
  switch (header[1]) { /* the different instruction types */
  case 0x70: length = 6; dir = OUT; break;
  case 0x72: length = 16; dir = IN; break;
  case 0x74: length = 32; dir = IN; data = msg; break;
  case 0x76: length = 1; dir = IN; break;
  case 0x78: length = 8; dir = OUT; data = seed; break;
  case 0x7a: length = 25; dir = OUT; data = display; break;
  case 0x7c: length = 16; dir = OUT; break;
  case 0x7e: length = 64; dir = OUT; break;
  case 0x80: length = 1; dir = IN; break;
  case 0x82: length = 64; dir = OUT; break;
  default:
```

```
  if (!passive) {
  send(''\x6d\x00'', 2);
/* unsupported instruction */
  hc = 0;
  } else sync_lost = 1;
  printf(''\rUnsupported instruction code %02x!\t\t\n'',
  header[1]);
  }
  if (header[2] != 0x00 || header[3] != 0x00) {
  if (!passive) {
  send(''\x6b\x00'', 2);
/* incorrect reference */
  hc = 0;
  } else sync_lost = 1;
  printf(''\rUnexpected P1 P2 values: %02x %02x!\t\t\t\n'',
  header[2], header[3]);
  }
  if (length != header[4]) {
  if (!passive) {
  send(''\x67\x00'', 2);
/* incorrect length */
  hc = 0;
  } else sync_lost = 1;
  printf(''\rIncorrect length %d in instruction
  %02x!\t\t\n'',
  header[4], header[1]);
  }
  if (hc == 5)
  if (!passive) {
/* procedure byte: no Vpp, send all data in one piece */
  if (send((char *) header + 1, 1)) continue;
  if (dir == IN)
  received = 0;
  else {
/* here comes the answer */
  if (send((char *) data, length)) continue;
  if (send(''\x90\x00'', 2)) continue;
/* ack: everything ok */
  if (debug) log_packet(header, data, OUT);
  hc = 0;
  received = -1;
  }
  } else {
  if (receive(&proc_byte, 1)) {
  if (sw2_next) {
  hc = 0;
  received = -1;
  sw2_next = 0;
  } else if (((proc_byte & 0xf0) == 0x60 ||
```

```
  (proc_byte & 0xf0) == 0x90) && proc_byte != 0x60)
  sw2_next = 1;
  else if (((proc_byte ^ header[1]) & 0xfe) == 0xfe) {
  printf(''\rSingle byte handshaking not suppor-
  ted!\t\t\n'');
  sync_lost = 1;
  }
  else if ((proc_byte & 0xfe) != header[1]) {
  printf(''\rUnexpected procedure byte %02x, INS =
  %02x!\t\n'',
  (unsigned char) proc_byte, header[1]);
  sync_lost = 1;
  } else {
  received = 0;
  sw2_ok = 0;
  }
  }
  }
  }
  } else if (received < header[4]) {
/* waiting for more data to receive */
  received += receive((char *) data + received, header[4] -
  received);
  } else if (!passive || sw2_ok) {
/* here, all data has been received */
  if (!passive)
  if (send(''\x90\x00'', 2)) continue;
/* ack: everything ok */
  if (debug) log_packet(header, data, dir);
/* reaction on received data */
  switch (header[1]) {
  case 0x72:
  if (debug) break;
  printf(''\nMessage from previous card:\n'');
  for (i = 0; i < 16; i++)
  printf(''%02x '', buffer[i]);
  printf('' '');
  for (i = 0; i < 16; i++)
  putchar((buffer[i] > 31 && buffer[i] < 127) ? buffer[i] :
  '.');
  putchar('\n');
  break;
  case 0x74:
  if (data[0] & 8) {
  if (vcl_in) {
/* lookup random number seed in VCL file */
  u = vcl_current + 1;
  if (u >= vcl_count) u = 0;
```

```
while (*(long *)(msg + 28) != vcl_msg_hash[u] &&
u != vcl_current)
if (++u >= vcl_count) u = 0;
if (u != vcl_current) {
vcl_current = u;
memcpy(seed, vcl_seed + u, 8);
display[0] = 0x80;
if (!debug && !economy)
printf(''\r\t\t\t\t\t\rMatched position %u.'', u);
} else {
memset(seed, 0, 8);
if (!debug && !economy)
printf(''\r\t\t\t\t\t\rNo match currently in VCL
file.'');
if (!economy && message) {
display[0] = '\xd8';
memcpy(display + 13, ''NO MATCH :-('', 12);
}
}
} else {
/* calculate random number seed from crypto message */
check = decode(msg, seed);
if (!economy) {
/* keep history of last LOGMAX crypto messages */
time(&logtime[lognext]);
memcpy(logmsg[lognext++], buffer, 32);
if (loglength < LOGMAX) loglength++;
if (lognext >= LOGMAX) lognext = 0;
/* manage on screen display */
if (station == 0) {
if ((check >> 2) == 1) {
/* it's a Sky channel */
if (data[6] != 0xd1) {
station = 1;
strcpy((char *) display + 13,
channel_id[data[6] & 0x0f]);
}
} else if ((check >> 2) == 2) {
station = 1;
strcpy((char *) display + 13, ''ADULTCHANNEL'');
} else if ((check >> 3) == 3) {
station = 1;
strcpy((char *) display + 13, '' JSTV '');
} else {
station = 1;
if ((data[0] & 0xe0) != 0xc0)
strcpy((char *) display + 13, ''NO KEY FITS!'');
}
} else if (station == 1) {
```

```
/* now remove on-screen display */
  display[0] = 0x80;
  station = 2;
  }
/* PC display message */
  if ((check >> 2) == 1) {
/* it's a Sky channel */
  if (data[6] != 0xd1)
  current_name = channel_name[data[6] & 0x0f];
  } else if ((check >> 2) == 2)
  current_name = ''Adult Channel'';
  else if ((check >> 2) == 3)
  current_name = ''JSTV'';
  else if ((data[0] & 0xe0) != 0xc0)
  current_name = ''???, no key fits'';
  if (!debug)
  printf(''\r\t\t\t\t\t\rDecrypting %s (%02x %02x %02x)'',
  current_name, data[0], data[1], data[6]);
  }
  if (check & 2)
  printf(''\nChecksum wrong !!!\n'');
  }
  }
  break;
  case 0x76:
  printf(''\rAuthorize button pressed.\t\t\t\t\n'');
  break;
  case 0x78:
  if (vcl_out && !suspended) {
  fwrite(msg + 28, 1, 4, vcl_out);
/* final 8 bytes of 74h cmd */
  seed[7] &= 0x0f;
/* only 60-bit are needed by decoder */
  fwrite(seed, 1, 8, vcl_out);
  vcl_count++;
  }
  break;
  default: break;
  }
  hc = 0;
  received = -1;
  } else {
/* wait in passive mode for SW1 and SW2 */
  if (receive(&proc_byte, 1)) {
  if (sw2_next) {
  sw2_ok = 1;
  sw2_next = 0;
  } else if (((proc_byte & 0xf0) == 0x60 ||
```

```
(proc_byte & 0xf0) == 0x90) && proc_byte != 0x60)
sw2_next = 1;
else {
printf(''\rUnexpected SW1 byte %02x, INS = %02x!\t\n'',
(unsigned char) proc_byte, header[1]);
sync_lost = 1;
}
}
} /* if (!passive || sw2_ok) else */
} /* if (hc < 5) else */
} /* while (!quit) */
deactivate_com();
printf(''\n'');
if (vcl_out) {
/* close VCL file */
buffer[0] = 0;
/* fill up file to a multiple of 1024, so that there are
* no undeleted bytes in final DOS disk clusters. */
for (l = 128 + vcl_count * 12; (l & 0x3ff) != 0; l++)
fwrite(buffer, 1, 1, vcl_out);
/* write number of seeds into header */
if (fseek(vcl_out, 4, SEEK_SET)) {
perror(''Sorry, can't fseek() in VCL file'');
exit(1);
}
putc((vcl_count >> 24) & 0xff, vcl_out);
putc((vcl_count >> 16) & 0xff, vcl_out);
putc((vcl_count >> 8) & 0xff, vcl_out);
putc(vcl_count & 0xff, vcl_out);
if (fclose(vcl_out)) {
perror(''Sorry, can't close VCL file!'');
exit(1);
}
}
return 0;
}
```

ASYNC.DOC

This is a set of rather simple serial communication routines written in assembly, and to be called from C. If it is not stated elsewhere, this code is public domain! Do with it as you wish, put it in your programs, etc, etc.

This is the second 'release' of the ASYNC functions. Since the first release several people have contributed modifications to the routines, to which I want to give them thanks and some credit where credit is due.

Roy M. Silvernail --
roy%cybrspc@cs.umn.edu - OR- cybrspc!roy@cs.umn.edu

For clarifying the documentation of AsyncHand() and AsyncSet(). He added a few #define's to further clarify AsyncSet(). He also is responsible for adding some error checking to AsyncInit()-- it now returns a non-zero on error (when the COM port isnt there).

Steve Miller -
uunet!pictel!miller

For finding a rather obscure bug. If a character was recieved and sent at exactly the same time, then it would stop receiving or sending characters.

Thanks again.

In addition, the buffer size has been increased from 1024 to 8196 characters.

Here is a list of all the files included in this package:

```
async.doc - What you are reading.
async.h - The C prototypes/header file
async.asm - The assembly source
term.c - The source for a simple terminal program
asyncs.obj - The .obj async.asm file for the SMALL model
asyncc.obj - The .obj for the COMPACT model
asyncm.obj - The .obj for the MEDIUM model
asyncl.obj - The .obj for the LARGE model
term.exe - The executable for the terminal program
```

I have used these with Turbo C, and Turbo ASM without any problems. It should work with Microsoft C and ASM, but a bit of re-writing will be needed

to make the assembler part work. I have also used it with Turbo C++ and Turbo Assembler 2.0 without any problem, but you will have to treat the Async functions as standard C, rather than C++.

Here is a short tutorial of the Async functions:

```
AsyncInit( int Port) AsyncStop( void) These functions
start and stop the interrupt handlers. No characters can be
recieved if it isn't started, and the computer will crash if
they are not stopped before the program is exited. The
paramater 'port' is the COM port to use, there are #defines
in the header file that defines the values to be used. It
would be 'more bug proof' if AsyncStop was called via the
atexit() function (check your compiler manual).

AsyncInit() will return a non-zero value upon an error
(when the COM port is not there).

AsyncClear( void) Clears the internal buffers.

AsyncOut( int c) Sends out a character.

AsyncIn( void) Returns the next character in the buffer or a
NULL upon an empty buffer. Use AsyncInStat() to check for
the number of characters in the buffer.

AsyncHand( int handshake) Sets the status of the handshak-
ing lines. The values are defined in the header file and can
be or'd together. A typical call would look like this:

AsyncHand( DTR | RTS);
```

Roy M. Silvernail found confusion in this rather simple explanation of AsyncHand(). I thought of editing the above description, but his description is better than mine, so here it is:

"The AsyncHand routine wants the whole set of flags upon invocation. At first, I had tried AsyncHand(~DTR) to drop DTR, but soon found it didn't work. With the 2 main control bits being DTR and RTS, AsyncHand(RTS) drops DTR just fine, and (of course) AsyncHand(DTR | RTS) raises it once again."

AsyncSet(int Baud, int Control) This sets the baud rate, paraty, etc, of the serial line. The paramater 'Baud' is the baud rate (ie 1200, 2400, 9600, etc),

and 'control' is a number that represents parity, length and stop bits. There are defines for this in ASYNC.H, but here are a few commonly used examples:

AsyncSet(2400, BITS_8 | STOP_1 | NO_PARITY) for 2400 baud 8N1.

AsyncSet(9600, BITS_7 | STOP_1 | EVEN_PARITY) for 9600 baud 7E1.

AsyncInStat(void) This frunction returns the number of characters in the input buffer.

AsyncOutStat(void) Returns the number of characters in the output buffer.

AsyncStat(void) Returns the status of the handshaking lines. Use the & and | oporaters with the values defined in the header file to extract any useful informaton out of this value.

The values used include the normal DCD, RI, and CTS, but also include D_DCD for 'Delta-DCD' or CHANGE IN DCD. This is useful in detecting changes in the handshaking lines since the last time the status was read.

These routines do have their limitations, however. They cannot deal with more than one serial port, and cannot take advantage of the 16550 UART. There is also no routines for input and output of strings-- there is so many ways of doing it that I left it up to whoever used these routines.

Enjoy, and if you have any questions, don't hesitate to ask.

David Kessner - dkessner@vigra.com - 1994-06-01

ASYNC.ASM

```
; interrupt driven serial port I/O module.
; written by David Kessner
; modified for MASM 5.1 compatibility on 1994-04-11 by WK

  EOI equ 020h  ; 8259 end-of-interupt
  Ctrl8259_0 equ 020h  ; 8259 port
  Ctrl8259_1 equ 021h  ; 8259 port (Masks)
  BufSize equ 8196  ; Buffer Size
  _DATA SEGMENT WORD PUBLIC 'DATA'
  assume cs:DGROUP, ds:DGROUP, ss:DGROUP
; Various things to be set upon AsyncInit()
  VectorNum db ? ; Vector Number
  EnableIRQ db ? ; Mask to enable 8259 IRQ
  DisableIRQ db ? ; Mask to disable 8259 IRQ
  VectorSeg dw ? ; Old Vector Segment
  VectorOfs dw ? ; Old Vector Offset
; Register Addresses for the 8250 UART
  Port  dw ? ; Port Base Address
  RegStart LABEL WORD
  THR  dw ? ; Transmitter Holding Register
  RDR  dw ? ; Receiver Data Register
  BRDL  dw ? ; Baud Rate Divisor, Low byte
  BRDH  dw ? ; Baud Rate Divisor, High Byte
  IER  dw ? ; Interupt Enable Register
  IIR  dw ? ; Interupt Identification Register
  LCR  dw ? ; Line Control Register
  MCR  dw ? ; Modem Control Register
  LSR  dw ? ; Line Status Register
  MSR  dw ? ; Modem Status Register
; Buffer Data
  RecBuffer db BufSize DUP (?) ; Recieve Buffer
  RecHead dw ? ; Buffer Head Pointer
  RecTail dw ? ; Buffer Tail Pointer
  TransBuffer db BufSize DUP (?) ; Transmit Buffer
  TransHead dw ? ; Buffer Head Pointer
  TransTail dw ? ; Buffer Tail Pointer
  ; Register Offsets for the UART
  RegOffsets dw 0, 0, 0, 1, 1, 2, 3, 4, 5, 6
  _DATA ENDS
  _TEXT SEGMENT WORD PUBLIC 'CODE'
  assume cs:_TEXT, ds:DGROUP, ss:DGROUP
  PUBLIC _AsyncInit, _AsyncClear, _AsyncStop
  PUBLIC _AsyncIn, _AsyncOut, _AsyncSet
  PUBLIC _AsyncHand, _AsyncStat, _AsyncInStat
```

```
  PUBLIC _AsyncOutStat
;---------------------------------------- ----------------------------
; AsyncClear   Empty the recieve buffer
;---------------------------------------- ----------------------------
; void AsyncClear( void);
;
;
;---------------------------------------- ----------------------------
  _AsyncClear PROC NEAR
  cli
  push ax
  mov ax, offset RecBuffer
  mov [RecHead], ax
  mov [RecTail], ax
  mov ax, offset TransBuffer
  mov [TransHead], ax
  mov [TransTail], ax
  pop ax
  sti
  ret
  _AsyncClear ENDP
;---------------------------------------- ----------------------------
; AsyncInit   Initalize Serial Port and install ISR
;---------------------------------------- ----------------------------
; void AsyncInit( int port)
;
; Where Port is
;  0 = COM1
;  1 = COM2
;  2 = COM3
;  3 = COM4
;
;---------------------------------------- ----------------------------
  _AsyncInit PROC NEAR
  CommPort equ bp+4
  push bp
  mov bp, sp
  ;---- Set various things according to com port number
  mov ax, [CommPort]
;----- COM1
  cmp ax, 0
  jne _AsyncInit_1
  mov [Port], 03F8h
```

```
  mov [VectorNum], 0Ch
  mov [EnableIRQ], 0EFh
  mov [DisableIRQ], 10h
  jmp _AsyncInit_Done
  _AsyncInit_1:
;----- COM2
  cmp ax, 1
  jne _AsyncInit_2
  mov [Port], 02F8h
  mov [VectorNum], 0Bh
  mov [EnableIRQ], 0F7h
  mov [DisableIRQ], 08h
  jmp _AsyncInit_Done
  _AsyncInit_2:
;----- COM3
  cmp ax, 2   ; 2
  jne _AsyncInit_3
  mov [Port], 03E8h  ; 03E8
  mov [VectorNum], 0Ch ; 0C
  mov [EnableIRQ], 0EFh ; EF
  mov [DisableIRQ], 10h ; 10
  jmp _AsyncInit_Done
  _AsyncInit_3:
;----- COM4
  mov [Port], 02E8h  ; 02E8
  mov [VectorNum], 0Bh ; 0B
  mov [EnableIRQ], 0F7h ; F7
  mov [DisableIRQ], 08h ; 08
  _AsyncInit_Done:
;---- Compute Register locations
  mov cx, 10
  mov bx, offset RegOffsets
  push di
  mov di, offset RegStart
  _AsyncInit_4:
  mov ax, [bx]
  add ax, [Port]
  mov [di], ax
  add bx, 2
  add di, 2
  loop _AsyncInit_4
  pop di
;----- Initalize Buffer
  call _AsyncClear
;--- Save and reassign interrupt vector
  push ds    ; Save Old Vector
  mov al, [VectorNum]
  mov ah, 35h
  int 21h
  mov [VectorSeg], es
```

```
  mov [VectorOfs], bx
  mov al, [VectorNum]
  push cs    ; Set New Vector
  pop ds
  mov dx, offset AsyncISR
  mov ah, 25h
  int 21h
  pop ds
;----- Enable 8259 interrupt (IRQ) line for this async adapter
  in al, Ctrl8259_1
  and al, [EnableIRQ]
  out Ctrl8259_1, al
;----- Enable 8250 Interrupt-on-data-ready
  mov dx, [LCR]  ; Read Line control register and clear
  in al, dx ; bit 7, the Divisor Latch Address
  and al, 07Fh
  out dx, al
  mov dx, [IER]
  mov al, 0 ; we're gonna test the UART first
  out dx, al
  in al, dx ; if this isn't 0, there's no UART
  cmp al, 0
  jnz _AsyncInit_222
  mov al, 3
  out dx, al
;----- Clear 8250 Status and data registers
  _AsyncInit_10:
  mov dx, [RDR]  ; Clear RDR by reading port
  in al, dx
  mov dx, [LSR]  ; Clear LSR
  in al, dx
  mov dx, [MSR]  ; Clear MSR
  in al, dx
  mov dx, [IIR]  ; Clear IIR
  in al, dx
  test al, 1
  jz _AsyncInit_10
;----- Set Bit 3 of MCR -- Enable interupts
  mov dx, [MCR]
  in al, dx
  or al, 08h
  out dx, al
;----- Clear Buffer Just in case
  call _AsyncClear
;----- Return
  xor ax, ax
  _AsyncInit_222:
  pop bp
```

```
  ret
  _AsyncInit ENDP
;---------------------------------------------- ----------------------------
; AsyncStop    Uninstall ISR
;---------------------------------------------- ----------------------------
; void AsyncStop( void)
;---------------------------------------------- ----------------------------
  _AsyncStop PROC NEAR
  push bp
  mov bp, sp
;----- Mask (disable) 8259 IRQ Interrupt
  in al, Ctrl8259_1
  or al, [DisableIRQ]
  out Ctrl8259_1, al
;----- Disable 8250 interrupt
  mov dx, [LCR]
  in al, dx
  and al, 07Fh
  out dx, al
  mov dx, [IER]
  xor al, al
  out dx, al
;----- Set bit 3 in MCR to 0
  mov dx, [MCR]
  in al, dx
  and al, 0F7h
  out dx, al
;----- Interrupts are disables. Restore saved interrupt vector.
  push ds
  mov al, [VectorNum]
  mov ah, 25h
  mov dx, [VectorOfs]
  mov ds, [VectorSeg]
  int 21h
  pop ds
;----- Return
  pop bp
  ret
  _AsyncStop ENDP
;---------------------------------------------- ----------------------------
; AsyncISR    Async Interrupt Service Routine
;---------------------------------------------- ----------------------------
; To be called only as an interrupt.
;---------------------------------------------- ----------------------------
  AsyncISR PROC NEAR
  push ax ; Save Registers
  push bx
```

```
  push ds
  push dx
  mov ax, @data  ; Address local data with ds
  mov ds, ax
  mov dx, [IIR]  ; Check if data actually received
  in al, dx
  and al, 06h
  cmp al, 04h
  je AsyncISR_recieve
  cmp al, 02h
  jne AsyncISR_end
;----- Transmit A byte
  AsyncISR_transmit:
  mov bx, [TransTail]
  cmp bx, [TransHead]
  jne AsyncISR_1
  mov dx, [IER]  ; Buffer empty
  mov al, 1
  out dx, al   ; Disable THR empty interrupt
  jmp AsyncISR_end
  AsyncISR_1:
  mov al, byte ptr [bx]  ; Get Byte
  inc [TransTail]  ; Update buffer pointer
  cmp [word ptr TransTail], offset TransBuffer + BufSize
  jb AsyncISR_2
  mov [TransTail], offset TransBuffer
  AsyncISR_2:
  mov dx, [THR]
  out dx, al
  jmp AsyncISR_end
;----- Recieve a byte
  AsyncISR_recieve:
  mov dx, [RDR]  ; Get Byte
  in al, dx
  mov bx, [RecHead]  ; Store Byte in buffer
  mov byte ptr [bx], al
  inc bx   ; Update RecHead
  cmp bx, offset RecBuffer + BufSize
  jb AsyncISR_10
  mov bx, offset RecBuffer
  AsyncISR_10:
  cmp bx, [RecTail]
  jne AsyncISR_20
  mov bx, [RecHead]  ; Cancel Pointer advance on overflow
  AsyncISR_20:
  mov [RecHead], bx  ; Store new pointer
  AsyncISR_end:
  mov al, EOI   ; Signal end ot interrupt
```

```
  out Ctrl8259_0, al
; Disable and re-enable interrupts so that there
; is an interrupt edge.
  mov dx,[IER] ; Point to Interrupt Enable Register.
  in al,dx ; Read the current value.
  push ax ; Save it.
  mov al,0 ; Disable the interrupts.
  out dx,al
  pop ax ; Restore original mask.
  out dx,al ; Re-enable interrupts.
  pop dx ; Restore saved registers.
  pop ds
  pop bx
  pop ax
  iret
  AsyncISR ENDP
;------------------------------------------- ----------------------------
; AsyncIn   Gets a byte from the input buffer
;------------------------------------------- ----------------------------
; int AsyncIn( void)
;------------------------------------------- ----------------------------
  _AsyncIn PROC NEAR
  push bp
  mov bp, sp
  xor ax, ax   ; Pre-Set result to 0
  mov bx, [RecTail]
  cmp bx, [RecHead]
  je _AsyncIn_return
  mov al, byte ptr [bx]
  inc [RecTail]
  cmp [word ptr RecTail], offset RecBuffer + BufSize
  jb _AsyncIn_return
  mov [RecTail], offset RecBuffer
  _AsyncIn_return:
  pop bp
  ret
  _AsyncIn ENDP
;------------------------------------------- ----------------------------
; AsyncOut  Output a byte
;------------------------------------------- ----------------------------
; void AsyncOut( int c)
;------------------------------------------- ----------------------------
  _AsyncOut PROC NEAR
  push bp
  mov bp,sp
  mov ax,[bp+4] ; get argument
  mov bx, [TransHead]
  mov cx, bx
```

```
  inc cx   ; Compute NEW buffer position
  cmp cx, offset TransBuffer + BufSize
  jb _AsyncIn_1
  mov cx, offset TransBuffer
  _AsyncIn_1:
  cmp cx, [TransTail]   ; Wait for space in buffer
  je _AsyncIn_1
  mov byte ptr [bx], al  ; Add byte to buffer
  mov [TransHead], cx   ; Update pointer
  mov dx, [IER]   ; Enable THR empty interrupt
  mov al, 3
  out dx, al
  pop bp
  ret
  _AsyncOut ENDP
;------------------------------------------------ ----------------------------
; AsyncSet  Set communication paramaters
;------------------------------------------------ ----------------------------
; void AsyncSet( int Baud, int Control)
;
; Baud = 150, 300, 600, 1200, 2400, 4800, 9600, 19200, 28800, 38400,
; 57600
; Control = The valure to place in the LCR
;------------------------------------------------ ----------------------------
  _AsyncSet PROC NEAR
  Baud equ bp+4
  Control equ bp+6
  push bp
  mov bp, sp
  mov bx, [Baud]
  cmp bx, 0
  je _AsyncSet_abort
  mov ax, 0C200h ; Baud rate divisor = 115200 / Baud
  mov dx, 0001h  ; 115200 = 0001C200h
  div bx
  mov cx, ax
  cli
  mov dx, [LCR]  ; Set Port Toggle to BRDL/BRDH registers
  mov al, 0ffh
  out dx, al
  mov dx, [BRDL]  ; Set Baud Rate
  mov al, cl
  out dx, al
  mov dx, [BRDH]
  mov al, ch
  out dx, al
  mov dx, [LCR]  ; Set LCR and Port Toggle
```

```
  mov ax, [Control]
  and al, 07Fh
  out dx, al
  sti
  _AsyncSet_abort:
  pop bp
  ret
  _AsyncSet ENDP
;------------------------------------------- ----------------------------
; AsyncInStat  Returns the # of characters in buffer
;------------------------------------------- ----------------------------
; int AsyncInStat( void)
;------------------------------------------- ----------------------------
  _AsyncInStat PROC NEAR
  push bp
  mov bp, sp
  mov ax, [RecHead]
  sub ax, [RecTail]
  jge _AsyncInStat_10
  add ax, BufSize
  _AsyncInStat_10:
  pop bp
  ret
  _AsyncInStat ENDP
;------------------------------------------- ----------------------------
; AsyncOutStat  Returns the # of characters in buffer
;------------------------------------------- ----------------------------
; int AsyncOutStat( void)
;------------------------------------------- ----------------------------
  _AsyncOutStat PROC NEAR
  push bp
  mov bp, sp
  mov ax, [TransHead]
  sub ax, [TransTail]
  jge _AsyncOutStat_10
  add ax, BufSize
  _AsyncOutStat_10:
  pop bp
  ret
  _AsyncOutStat ENDP
;------------------------------------------- ----------------------------
; AsyncHand  Sets various handshaking lines
;------------------------------------------- ----------------------------
; void AsyncHand( int Hand)
;------------------------------------------- ----------------------------
  _AsyncHand PROC NEAR
  Hand equ bp+4
```

```
  push bp
  mov bp, sp
  mov dx, [MCR]
  mov ax, [Hand]
  or al, 08h   ; Keep interrupt enable ON
  out dx, al
  pop bp
  ret
  _AsyncHand ENDP
;------------------------------------------------ ----------------------------
; AsyncStat  Returns Async/Modem status
;------------------------------------------------ ----------------------------
; unsigned AsyncStat( void)
;
; MSR is returned in the high byte, LSR in the low byte
;------------------------------------------------ ----------------------------
  _AsyncStat PROC NEAR
  push bp
  mov bp, sp
  mov dx, [MSR]
  in al, dx
  mov cl, al
  mov dx, [LSR]
  in al, dx  ; LSR in low byte
  mov ah, cl  ; MSR in high byte
  pop bp
  ret
  _AsyncStat ENDP
  _TEXT ENDS
  END
```

VideoCrypt-S

VideoCrypt-S was developed by News Datacom, Thomson and the BBC. The primary user of the system is the BBC Select service. This is an after hours pay television service. It carries varied programming from medical programming to business advisory programming. Above all these programmes are intended for audiences who are willing to pay.

The time slot of the programming holds its own special problem. Since the programmes were being aired after the main channels had closed down, most of the potential viewers would be asleep. Therefore it was necessary to include a timing circuit so that the programme could be videotaped for later playback.

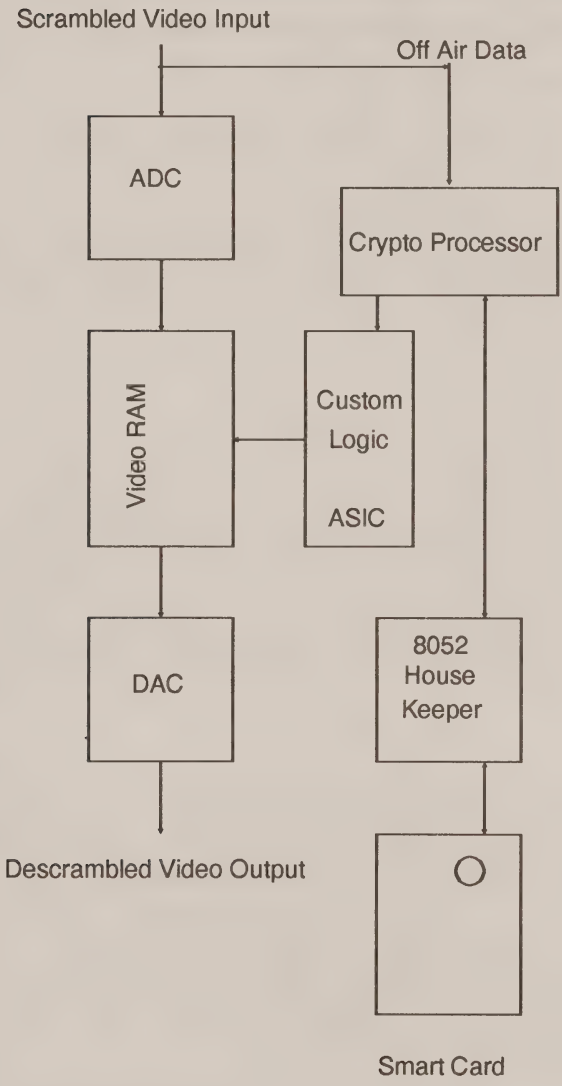
The cut and rotate technique of scrambling can send shivers down the spines of cable television engineers. The main technique of cable distribution relies on transverting an off air-signal and sending it through the cable network. In some larger nets, the signal is demodulated first and then remodulated and upconverted for distribution.

The weakness of a cut and rotate system is tilt. That it where the join points on the descrambled signal do not exactly match. This results in a lot of low frequency noise and glitching. The non-linearities on a cable system will accentuate this tilt problem. VideoCrypt has overcome this tilt problem and the satellite transmissions are relatively clean. On a cable system, the signal environment is controllable. The main amplifiers are temperature controlled as well as being gain controlled. The BBC Select service faced a different problem. The signal was to be distributed terrestrially via UHF transmitters.

System Operation

Line shuffle is where the order of a block of lines is changed. Line 1 might become line 10 in the scrambled order. The lines would then be restored to their proper order. This sounds simple but it is complex in reality.

VideoCrypt-S Architecture



The VideoCrypt-S system is based on a block scramble. Each block is forty seven lines with six blocks per field. The other lines in each field are reserved for teletext, VBI and access control data.

There are three scrambling modes available:

Full Shuffle 282 Lines

Half Shuffle - Every other field is shuffled

Clear Video Delay

The full shuffle and the half shuffle effectively destroy the picture. The block delay is not as secure as Discret has shown. When the modes are all used at the same time the effect on the picture is impressive. The clear block delay can outline the block and make analysis easier.

Access Control:

The access control system is based on the VideoCrypt system. Therefore it is smart card based. The scrambling is governed by a permutation generator. The seed for the generator is a 20 bit word derived from data transmitted over the air in an encrypted form.

The smart card holds the entitlement data, the user profile and the decryption algorithm necessary to decrypt the over the air data. In this respect it is the same as the ordinary VideoCrypt smart card.

Decoder Circuitry:

The main difference between VideoCrypt-S and VideoCrypt is the type of scrambling technique. VideoCrypt-S uses line shuffle and therefor requires a greater RAM storage. The shuffle is controlled by an ASIC. This ASIC was developed by Thomson.

According to an official paper on the system, the ASIC is the heart of the system. The ASIC handles the data extraction, the memory allocation and the permutation generation. The data is extracted from the VBI lines and processed. Then it is fed to the decoder microcontroller bus.

The housekeeper microcontroller in the VideoCrypt-S decoder is an 8052. According to sources, the program is unprotected and not dissimilar to that in the 8052 in the ordinary VideoCrypt decoder. The video ADC and DAC stages are similar to those of the ordinary VideoCrypt decoder.

Will VideoCrypt Hacks Work?

Some of the hacks that worked on VideoCrypt will work on VideoCrypt-S. The EPROM card write voltage hack will work but only if that type of card is employed. This is unlikely as Sky were so badly burned on this one that they had to bring out a new card issue to stop the hack.

Since most of the program in the 8052 housekeeper microcontroller is the same as that in the ordinary VideoCrypt, it is probable that this hack will work. It remains to be seen if the BBC Select smart cards are as clever as those of Sky 07 issue. If the BBC Select cards are 06 issue types then the KENtucky Fried Chip hack will work.

The smart cards used by the services are could probably be hacked if there was a demand. Of course here lies the most important question. There is no point in commercially hacking a system only to find there is no demand for the hack. The programming on the BBC Select service is not in widespread demand. Perhaps this factor will protect the service from any serious hacking.

References:

Hack Watch News - Various Issues

IBC Technical Papers 1992: BBC Select: A Terrestrial Subscription Television Service. The BBC Select Decoder

Cryptovision

The Cryptovision system is one of the newer entries to the European satellite television market but it has been around since the mid eighties. Its primary application to date has been as a cable based scrambling system.

Unlike many of the systems of that era, it has not been hacked. This is due mainly to the secure design of its access control system and the fact that it is not widely in use on satellite television. There are a number of companies examining the potential for hacking it due to the fact that Cablelink and SSVC use it.

The system is manufactured by Tandberg. Tandberg have been associated with pay television systems for a long time and they were among the first to launch MAC encoders and decoders.

It is currently in used on the British Services Channel which broadcasts via the Intelsat at 27.5 Degrees West. At first glance many expected the channel to be using the VideoCrypt system. This mistake arose from the fact that the system uses the same basic technique as the VideoCrypt system though the access control is totally different.

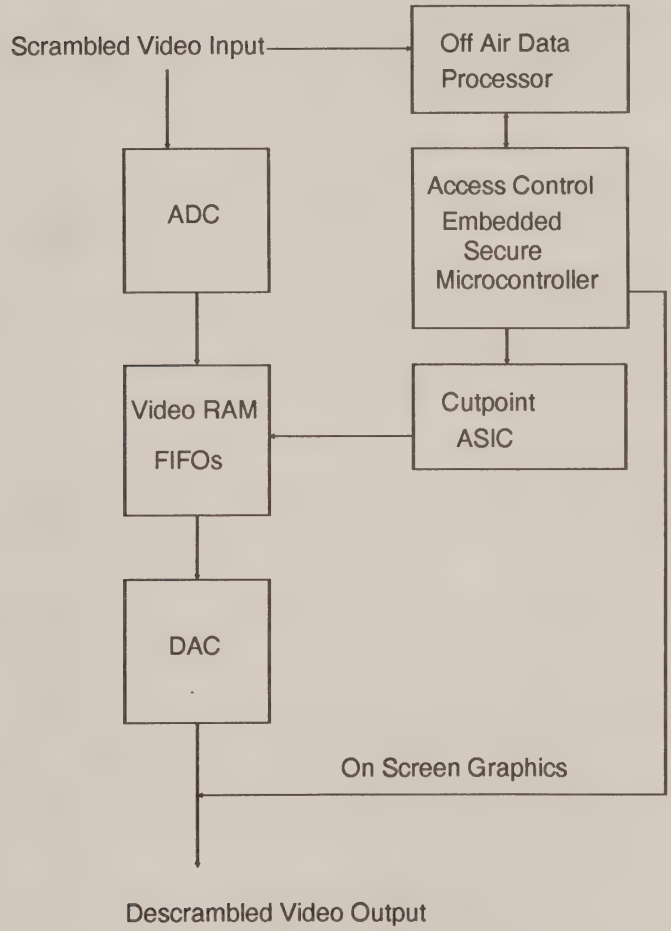
The system is not limited to satellite usage. Cablelink use it on the second largest cablenet in Europe, (260,000 Homes). It is used terrestrially in Scandinavia and Gibraltar. It is also being used in terrestrial rebroadcast applications such as MMDS in Ireland.

Video Scrambling

The technique used in the Cryptovision system is "Cut And Rotate". The line video is sectioned and cut, then rotated about the cut point. The sample rate is higher than the VideoCrypt system and as a result the quality of the descrambled picture is somewhat better.

The cutpoint in each line is masked effectively so that there is no transient at the point. One of the first attempts at hacking the VideoCrypt system used an inductor to accentuate the cutpoint. With masking this cutpoint disappears. Apparently the masking process involves a form of oversampling where the sample windows are longer than is required.

Cryptovision Decoder Architecture



The original specification used Digit 2000 series ADCs and DACs. It is now believed that they would use the TDA8702 and the TDA8703 ICs. The sampling frequency is 17.73 MHz or four times the PAL colour subcarrier frequency. This gives an improved picture quality.

Like the VideoCrypt system, there are 256 cutpoints each line. This is from a total of 921 samples. Some of the samples are not used. This makes it harder to detect the cutpoints in the scrambled video.

The Access Control System

The access control system is designed to be flexible in that it can support a number of methods ranging from over the air addressing to smart cards.

The vertical blanking interval carries the necessary crypto data and validation levels in an encrypted format. The data is virtually the same as teletext though it does not use the teletext lines. The use of a teletext like data format enables the use of cheap teletext ICs.

It is possible for the system user to switch on decoders over the air. It is this facility that makes the piracy on the system so difficult. The critical information is held in application specific integrated circuits in ROM and RAM. Any attempt to examine the RAM would destroy key data.

It is not definitely known what crypto system is used to encode the over the air data but it is possible that it is a DES variant. This would mean that an approach along this line would be tricky if not totally uneconomical. Even in the United States where the VideoCipher system uses the DES algorithm, the algorithm itself has not been reversed. There was a weak link in the access control section of that system that was exploited by hackers. Cryptovision have examined that hacks on VideoCipher and have no doubt hardened their system against a similar hack.

Audio Scrambling

There is an audio scrambling facility on the Cryptovision decoders though it has not yet been used. There are apparently a number of options and the following have been mentioned: encrypted adaptive delta modulation, encrypted NICAM and spectrum inversion.

Nagra Kudelski Syster

The Syster system was developed to replace the totally hacked Discret system. Canal Plus run the biggest network of channels in Europe and in France alone have over three million subscribers. Even though piracy is very much illegal, it has not completely deterred people from using pirate descramblers.

The actual scrambling system was created by Nagra Kudelski of Switzerland. The decoders are manufactured by Eurodec. Eurodec is jointly owned by Canal Plus and Sagem.

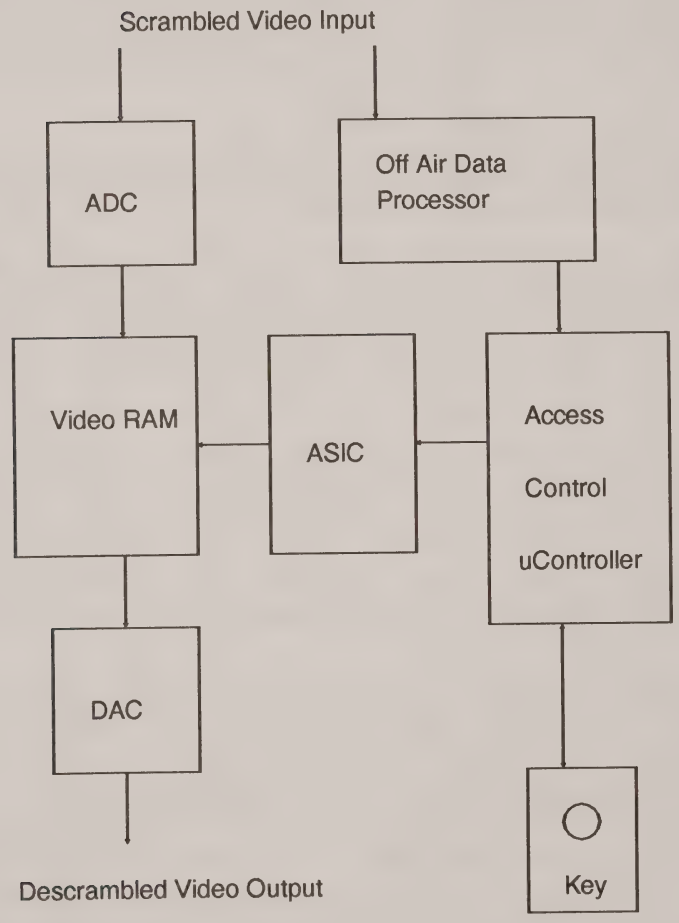
Most hackers refer to the system as the Nagra Kudelski Syster system or Nagravision or just as the Nagra Kudelski system. One of the reasons for this appears to be that the spelling of Syster looks like the spelling used for the name of a heavy metal band. Of course the actual name could have been a joke by the system developers. It is a real head banger to hack.

To date the system has been used on Canal Plus, Premiere and Canal Plus Espanga. Teleclub has also changed to the system. It will effectively become the de-facto German language scrambling system. The fact that Canal Plus in France are also using it makes it the most widely used system in Europe. According to sources, the system is being considered by the European Broadcasting Union for use on its newsfeed network.

The basic line shuffle appears to be in use on the Premiere feed on ASTRA whereas the combined shuffle and cut and rotate appears to be be used on the Spanish operation.

Unlike other systems, there appears to be a dearth of IRDs. In fact according to a few sources there are no integrated receiver decoders for Syster. The actual distribution of the decoders also appears to be controlled. This is one of the strengths of the system. It allows the programme provider to maintain control over the system. When IRDs are allowed then the programme provider loses control and Grey Market Piracy becomes a serious problem. The best illustration of this fact lies in what happened with VideoCrypt and Sky.

Nagra Kudelski Syster Architecture



The Video Scrambling

Syster is a chameleon system. It uses line shuffle scrambling in addition to line video cut and rotate. Other facilities such as line delay are believed to be present. This makes it the most formidable video scrambling section to hack.

The line shuffle technique has two forms. The fixed form is where the field is broken up into a number of bars having the same number of lines. The shuffle action takes place within the confines of the bar.

The sliding bar is a more secure form. Instead of the bar appearing at fixed positions in each field, the position of the bars change from field to field. This reduces the chances of success for a correlation hack that samples and compares fields.

The video descrambling process is, like most line shuffle systems, ASIC based. Since this ASIC has to handle the line cut and rotate as well, it would have to be one of the most advanced in any decoder.

The architecture of the video descrambling would be similar in some respects to that of VideoCrypt-S. A video ADC would digitise the scrambled video. The ASIC would route the digital video to the video memory and then would reconstruct the line sequence and where necessary derotate the line video segments.

A video DAC would then convert the descrambled digital video back to analogue. The descrambled video would then be filtered before being routed back to the receiver SCART.

The Access Control System

The access control system on Syster is a dual system. It uses over the air addressing in addition to a smart card or rather smart key. The carrier of the detachable secure microcontroller is key shaped. It is referred to as the "Key" on the advertising brochures.

The Key is reprogrammable over the air and is intialised when the subscriber is authorised. Apparently all Syster decoders have to be authorised over the air. The subscriber has to request the authorisation centre to authorise the decoder.

The over the air addressing is carried in the VBI. It has a fast data clock and is believed to be in the region of 4 MHz. This would give the system a fast subscriber update speed.

Hacks On Syster?

There have been rumours of hacks on the Syster system but to date there has been nothing approaching the magnitude of the D2-MAC or VideoCrypt hacks.

Some of the rumours mention a pirate version of the key card. However the main problem in such a potential hack is the acquisition of a suitable number of decoders. This is the point at which the VideoCrypt system designers demonstrated a complete ignorance of strategy.

The only way to maintain security on a system, even in the event of a hack, is to maintain control over the decoders. If there are no decoders then there will be no way short of designing and building a third party decoder that will allow the hack to continue.

The Syster decoders are not, as far as is known, integrated into IRDs. They are stand alone decoders. This means that each decoder could be, well theoretically at least, accounted for.

One unconfirmed report dealt with a dual PCB unit that worked as a pirate decoder for Syster. The boards were manufactured separately and when the user connects them together it works. At this point in time it is not known if this approach relies on a clone master situation or a genuine video hack.

The over the air data rate on Syster is high and as such it is not as vulnerable to the DDT hack as is VideoCrypt. However if some method of synchronisation on a recordable channel was used then DDT might be possible.

Other hacks such as Data Snatch Replay hacks could affect this system, as indeed they would do so for any card based system. If the authorisation sequence for a key card was recorded (as is typically done in VideoCrypt hacks) and then replayed after the card has been deactivated it would theoretically reactivate the card. Of course the card may well be killed again. Such a hack would require very careful analysis of the card authorisation and deauthorisation protocols. It also requires an understanding of how the access control system in Syster is constructed. Similar hacks on VideoCrypt rely on the fact that that system works on the Exclusion Principle. Kill signals are sent to knock cards out. If Syster works on the Inclusion Principle, where a heartbeat signal must be received by the card, a DSR may not work well if at all.

DECTEC's SUN

There are basically two types of recently designed addressable scrambling systems in use. The first type is the embedded secure processor type. The second is the detachable secure processor type. VideoCipher II was of the first type.

The best example of the second type is the Sky VideoCrypt system. The use of the detachable secure processor, ie the smart card, makes piracy difficult. It also means that the manufacture of the actual descrambler can be undertaken by subcontractors who will be supplied with the necessary ICs. The programming and the distribution of the smart card always remains under the programme provider's control. In the present piracy environment, an embedded secure processor approach can be fatal.

It is inevitable that what was secure five years ago will be easily hacked today. What appears to have happened in the case of VideoCipher II is that a group of non-techs have tried to regulate the progress of technology by trying to use the law to their advantage. To date they seem to have been effective. The reason being that the USA is a very litigious nation.

SUN - How It works

The US market is different from the European market in that VideoCipher II is the main and perhaps de-facto scrambling system. The people at VideoCipher wandered around for years thinking that nobody could duplicate their system.

Naturally when DECTEC, a Canadian company, emulated their system the people at General Instrument / VideoCipher went bananas, in fact they totally freaked out. Being bureaucrats, this event naturally sent them scurrying to get their lawyers to attack DECTEC. An attack which failed thanks to the rare sanity of law.

The SUN decoder differs from other descramblers on the market in that it is totally reconfigurable. This means that the decoder can be used to descramble VideoCipher II or OAK ORION or B-MAC. It merely requires the correct software. This versatility has caused some problems.

The key phrase in use here is "emulate". This allows the circuitry to be configured to descramble a particular system. It does not mean that the system is actually a descrambler for that particular system. This is a common practice in the computer industry.

VideoCipher II system is the de-facto system in the United States even though it has massive piracy problems. The manufacture of the VideoCipher II units is a monopoly situation for GI and they are loathe to relinquish this.

It would appear that the prevalent situation in the US is that engineering companies are being run by lawyers rather than lawyers by companies. This is unfortunate as a mere hired mouthpiece should not be allowed to dictate the run of creativity. If this trend continues in the US, there will not be any electronics industry left.

The SUN decoder is intended to be a vanilla system that can be configured to emulate any scrambling system given the correct configuration and authorisation software. The SUN stands for Secure Universal Norm.

The SUN Architecture

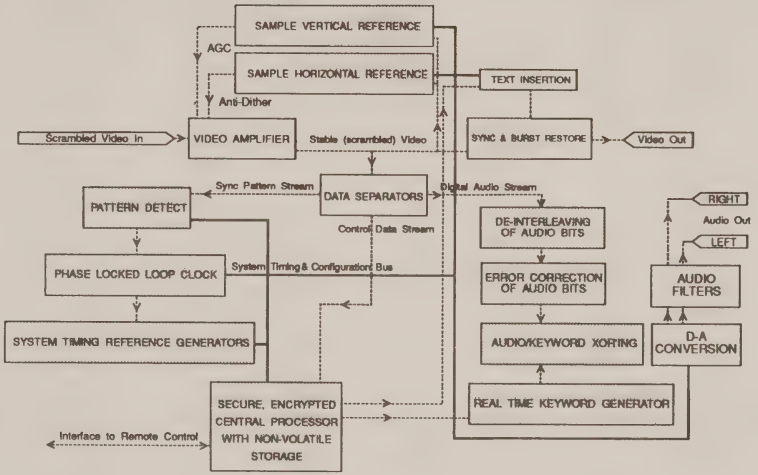
The central element in the SUN decoder is the Xilinx Field Programmable Gate Array. This is a product designed by Xilinx of San Jose in the United States.

The standard procedure when designing descramblers is to integrate as many functions on to large scale integration ICs. Generally the designers will use a gate array IC to house most of the housekeeping logic. This is perhaps one of the greatest weaknesses of a "frozen" architecture system. The design, once implemented, either cannot be altered or can be altered with extreme difficulty. This is where the benefits of the FPGA become apparent.

The Field Programmable Gate Array allow the design architecture to be updated or reprogrammed in the field. This makes it ideally suited to use in scrambling systems.

The design process is straightforward. The design is inputted by the designer into a computer program called XACT. This program then evaluates and optimises the circuit in terms of design structure and propagation delays. When this is completed, the XACT program generates a bitstream that can be downloaded into the FPGA chip.

SUN System Architecture



Shaded portions are re-programmable and configured by central processor every time power is applied. Therefore all these functions can be modified in the field.

Non-shaded portions are analog and require switched levels if multiple systems are to be emulated. Therefore, these primitive functions must be decided on at manufacture.

The bitstream goes to a static RAM memory on the the FPGA. This is the configuration data for the FPGA. Since this is static RAM, the contents are lost on power down. The contents can be maintained by a battery backup or can be stored in ROM or in a SMART card. In addition, the number of times that the data can be read back for verification can be set. Therefore it is possible to verify the data once and lock out any prying eyes.

The architecture used in the Xilinx FPGA is known as "Logic Cell Array". This is structure in which an array of inner logic cells are surrounded by input - output interfaces blocks. The logic cells are composed of combinational and sequential logic circuitry .

As can be seen from the SUN System Architecture map, the decoder is basically two sections. There is the standard fixed section and the reconfigurable section.

While the fixed section is for the most part analogue, it does contain the digital audio converters used for the digital audio section. The fixed section must be decided upon at the time of manufacture.

The primary market for the first SUN decoders is the United States. This means that the systems that the SUN will initially emulate are the VideoCipher II, the VideoCipher II Plus and the Oak ORION systems.

The above systems are Soft Video - Hard Audio types. The video scrambling on all of the above systems is, in European terms, simple. The audio on these systems is digital and hard encrypted. The VideoCipher audio is encrypted using DES. The OA K ORION uses a digital compression that is in some ways similar to NICAM along with an encryption process.

The SUN decoder is essentially a vanilla audio and video descrambler. The systems descrambled depend on the control data in the Xilinx FPGAs. There are a number of ways of setting up the SUN decoder. The first and most obvious is a personality board.

The term "personality board" is a common one in bare metal computer circles. It generally describes a board or card that allows a computer to emulate the technology of another computer in order to run programs written for that computer. The best example would be the PC emulators for the Atari and Commodore computers.

The personality board is generally one or more microcontrollers that have been programmed to load data in the FPGAs on power up. There still is a requirement for the decoder to be authorised by the service supplier.

When DECTEC developed the SUN decoder, they proved that it was possible to emulate the VideoCipher II decoder operation. The personality board used in this instance was based on the 87C series of microcontrollers.

As with the European market, the latest trend in the US is towards SMART cards. Even General Instrument strangely announced their entry into the field. DECTEC are currently testing a SMART card based unit. This will allow the decoder to be configured from a SMART card. This card type is different from the card used by the VideoCrypt system and is more secure. It is believed that it will be based on one of the Dallas type cards.

The SUN decoder can be applied to other scrambling systems such as the B-MAC system or indeed the VideoCrypt system. In either case it will have to be authorised. In the case of B-MAC, certain custom logic chips would have to be incorporated into the SUN decoder design.

It should be stated that DECTEC is not a pirate company. Their aim is to supply a unit that is capable of bringing some sense into a rather chaotic market. The SUN decoder has some strong possibilities that would make it usable here in Europe. The decoder can be applied to the MAC systems. It is not impossible that we may see a SUN decoder that is capable of handling VideoCrypt, Nagravision, Eurocrypt and maybe FilmNet's digital audio.

The primary advantage of the SUN decoder is that it is totally reconfigurable and agile. This means that the descrambler structure itself can be changed in the event of the system being compromised. This is a most powerful tool for any scrambling system.

Any system that has a "frozen" architecture will at some stage be hacked. A "frozen" architecture is one that has been implemented in custom IC design or Application Specific ICs. Some people consider it a defence that the key sets in a "frozen" architecture system can be reprogrammed. This kind of logic is characteristic of those who do not understand the pirate mind. Perhaps that is because they have only had a one-sided experience of piracy - as a victim!

Digicrypt

The Digicrypt system started out as the Sat-Tel VideoCode system. DCE took over the business interests of Sat-Tel when Sat-Tel liquidated. VideoCode was one of the main developments.

The system was a joint development between Zenith (USA) and Sat-Tel / DCE. Zenith provided the over the air access control system and software and the hardware was developed by Sat Tel. It had been demonstrated at the International Broadcasting Convention 1990 and at various Cable And Satellite Shows. There have been no reports of the system actually being deployed yet.

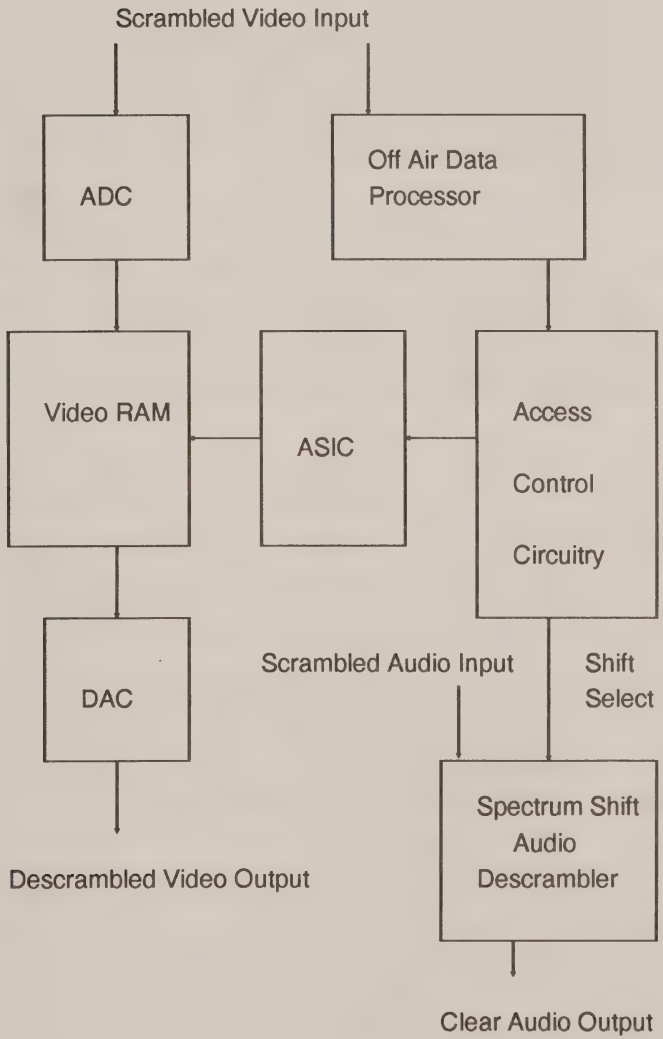
Video Scrambling

There are two techniques used in the Digicrypt; line delay and line shuffle. The line delay appeared on demonstration to be a single unit delay. The demonstration in question was at the IBC. This facility is not mentioned in the Digicrypt literature issued by DCE. There are two possibilities. Either the facility has been dropped or it is a reserve facility. Judging from the amount of critical information given in the literature it is a reserve facility. It would also follow that DCE appears to be new to the signal security business. The literature contains very little of the generalities used on other system brochures.

The line shuffle used is either a 32 line shuffle or a 128 line shuffle. With this low line count, the shuffle type is probably the sliding bar type.

The video decoder architecture would be similar to most other line shuffle based decoders. The main difference would be in the access control section. This could be an outboard provided by Zenith and would, if this was the case, be housed in a pluggable module similar to the BSB EuroCypher ACM. Alternatively, since Zenith were involved from such an early stage, the access control section could be part of the actual main PCB.

Possible Digicrypt Block Diagram



Audio Scrambling

The audio scrambling used is the same as that used by the BBC on the Intelsat at 27.5 Degrees West. After all, Sat-Tel manufactured those descramblers and the audio scrambling was developed by Sat-Tel.

Now for the critical data. The audio scrambling system, according to the data sheet is an upward spectrum shift. The range of the spectrum shift is from 170 Hz to 3.1 KHz. In other press releases included in the same folder, they state that the AudioCode system is capable of 12 different frequency shifts.

Access Control

The access control system used by Digicrypt is an over the air type. Four lines of the VBI are used to transmit the addressing data. The system can address up to 9000 decoders per minute.

The number of decoders that can be addressed on one system is 16.7 million. The tier structure is 256 levels wide.

Hacks

Since this system has not been deployed, this would be a hypothetical hack. The video scrambling is too secure to hack and obviously is not the weak point. The weak point would be found in the access control system to descrambler interface.

Most of the circuitry would be ASICed to counter such a hack. There is the possibility that the Zenith system would be related to previous versions in the United States. Therefore a comparison of the systems would be in order. If there is a great enough use of the system then, the ASICed areas will be reverse engineered.

Multiplexed Analogue Component.

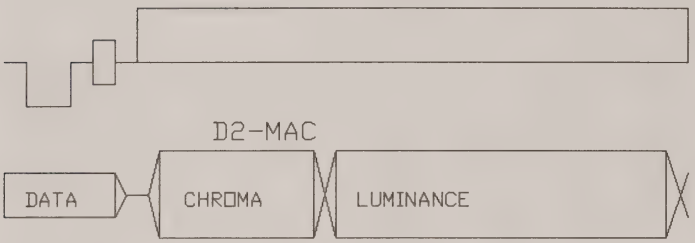
At a meeting in 1977, the World Administrative Radio Council, (WARC), formulated the guidelines for Direct Broadcast via Satellite. No transmission standard was recommended. There were a number of transmission standards developed in the early eighties for DBS. The two front runners were Extended PAL, (E-PAL) and Multiplexed Analogue Component, (MAC). Unfortunately DBS did not evolve as WARC 77 envisaged. In fact it would seem that the world just ignored the WARC. Considering that the main people involved were civil servants and members of monopoly PTTs that was probably a good thing.

The EC bureaucrats decided on the MAC system. It is a good system but it is the wrong answer from a technical point of view. Their motives were right. By choosing MAC, the EC put the Japanese at a disadvantage. European firms are now in the lead in MAC technology.

The MAC system transmits the luminance and the chrominance separately. Both are time compressed. The compressed components are then transmitted sequentially. The components are expanded and combined to give YUV or RGB at the receiver using digital techniques.

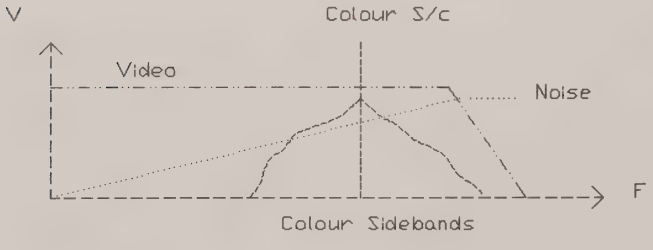
The compression of the video information allows greater depth for audio and teletext services. The line synch in the PAL system is transmitted as a pulse in each line. The pulse takes a considerable amount of the actual line time. With the MAC system, the line synch can be derived from a six bit synch word in the data block.

MAC has a specific advantage over PAL when used in a satellite channel. In a frequency modulated system, the noise voltage to frequency response is triangular. The noise voltage rises almost linearly with frequency. In the PAL signal, the colour or chrominance information is mainly in the upper section of the baseband signal, (3.5MHz to 5.5MHz). As a result, the highest noise voltage appears in the chrominance producing a lower signal to noise ratio. Pre-emphasis only offers slight compensation for this effect. De-emphasis can have one disadvantage when dealing with a near threshold PAL signal. Dot sparklies become streak sparklies due to the response of the de-emphasis network.



MAC offers a considerable saving in the time taken for elements such as synch. In the PAL waveform, the synch occupies a major section of the line. The horizontal blanking takes up just over a fifth of the total line time.

In the MAC signal, the chrominance is compressed by 3:1 nd the luminance is compressed by 2:1. This leaves the 10uS synch area to be occupied with data.



The noise in an frequency modulated PAL channel increases triangularly with frequency. As can be seen from the diagram, the noise is worst in the colour section of the spectrum.

There are a number of MAC variants. Some of these variants have fallen into disuse. The most common variants in use are B-MAC, D-MAC and D2-MAC. C-MAC is still used by NRK in Norway.

MAC Variants

A-MAC

This was the first version of the MAC family. The audio on this variant was on a 7.16 MHz subcarrier. It is not in use any more. It was essentially the prototype MAC system.

B-MAC

This version of MAC uses line delay as the video scrambling element. This is achieved by varying the length of the data packet. The data modulation format is 2-4 PSK. It is used by the AFRTS and the SIS Racing Channel.

C-MAC

This is the original EBU MAC specification. Frequency modulation was used for the video section of the line. Phase modulation was used for the data packet. It require two demodulators at the receiver. Its bandwidth limited it to satellite broadcast use only. The 27 MHz required bandwidth was too large for cablenets.

D-MAC

This system was used by the BSkyB, (previously British Satellite Broadcasting), satellite at 31 Degrees West. The D-MAC system can carry up to eight 15 KHz audio channels. It uses duobinary encoding of the data to reduce the required bandwidth on a cablenet to approximately 10.5 MHz.

This is still too wide for most European cablenets. This resulted in the D-MAC standard becoming a uniquely English standard. The rest of Europe chose D2-MAC.

D2-MAC

This variant is a subset of D-MAC. It has half of the audio capacity of D-MAC. As a result, it can fit in a bandwidth of a cablenet channel of 8 MHz. This is the most widely used MAC variant. There are two standards used for encryption on D2-MAC; Eurocrypt M and Eurocrypt S.

S-MAC

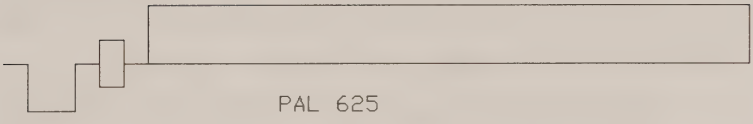
This variant is not used in broadcast applications due to the large bandwidth. It is also known as Studio MAC. The Y component is compressed by 2:1 and the U and V components by 4:1 respectively. This allows the multiplex to be carried on an ordinary PAL or NTSC line space complete with standard synch pulses. Its primary users are US studios.

Scientific Atlanta B-MAC

Scientific Atlanta's B-MAC is currently in operation on the Europe's largest private network - the Satellite Information Services' Racing Channel. The Racing Channel is supplied to a network of bookie's shops. There are four users of the system, Ladbrokes, William Hill, Coral and Mecca. Each user has its own audio channel and the teletext service gives the results.

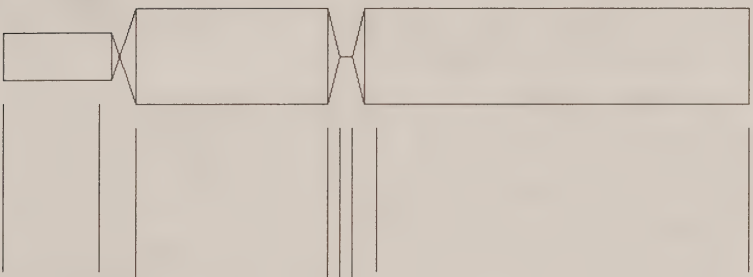
British Telecom initially supplied the decoders and receivers to SIS. The decoders were recognisably Scientific Atlanta but there was some question as to the origin of the receivers. The receiver was reverse engineered and turned out to have been manufactured by JRC. Apparently a separate production line had been set up by JRC for these receivers.

The receiver differed from other receivers of the period. The receiver's baseband had been widened to take the B-MAC signal and the baseband response had been widened to 10 MHz and the response had been smoothed. There was also an integrated receiver decoder version.



PAL 625

B-MAC



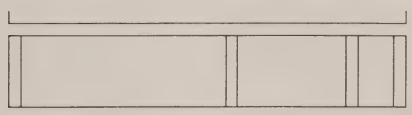
DATA
234
11uS

CHROMA
375
17u625

LUMA
750 SAMPLES
35u25

LUMA - CHROMA TRANSITION
6 SAMPLES
0u2

Data block varies from 75 to 45 symbols



2 45 2 20 2 5 2 SYMBOLS

EACH SYMBOL IS THREE SAMPLES WIDE

There are two versions of B-MAC, the 625 version as used in Europe and Australia and the 525 version as used in the USA and Canada. The architecture of the decoders is similar and in most areas identical. The primary differences are in the system clock rate and the central microcontroller.

The main application of the B-MAC system appears to be narrowcasting rather than broadcasting. It is commonly used for high pay services such as sports events. It is also used on some of the intra-company video conferencing links. One of the factors in this has been the relatively high price of the decoder.

In the United States and Canada, B-MAC has been mainly used on high pay services. The US variety has been totally hacked. It is possible to purchase replacement chips and out-boards that will give access to various high fee channels.

The B-MAC system is an old system. It reflects the scrambling technology of the mid eighties. Whereas the D2-MAC and D-MAC scrambling systems use cut and rotate, the B-MAC system uses a form of active line delay. In light of developments in hacking, this type of scrambling is now woefully inadequate.

It would be technically feasible to build a video only descrambler for under £200 using existing technology. Of course Scientific Atlanta are continually upgrading their system.

The audio modulation is Adaptive Delta Modulation (Chapter 4). The digital audio and control data occupies the first 11 uS of the waveform. At the maximum, the data is 75 symbols wide and the minimum is 45 symbols wide. So by varying the amount of data in the waveform the starting position of the video is varied.

The basic operation of the B-MAC system is similar to other MAC systems in that each line has three packets; data, chroma and luma. The time division multiplexer works in sample durations of 47nS. This roughly equates to 1365 samples per line (64 uS). D2-MAC differs from this in that it has only 1296 samples per line.

The sample frequency and sample allocation for each B-MAC line is as follows:

625 Line B-MAC

Sample Clock Frequency: 21.328 MHz (est)

Luminance: 750 Samples 35.165 uS

Chrominance: 375 Samples 17.582 uS

Luma-Chroma Transition: 6 Samples 0.281 uS

Data: 234 Samples 10.971 uS

525 Line B-MAC

Sample Clock Frequency: 21.479 MHz

Luminance: 750 Samples 34.918 uS

Chrominance: 375 Samples 17.459 uS

Luma-Chroma Transition: 6 Samples 0.279 uS

Data: 234 Samples 10.894 uS

Data Structure And Format

The modulation format used is Differential Quadrature Phase Shift Keying, (DQPSK). This format is covered in Chapter 4 in the NICAM section. From this point on the values used are for 625 line B-MAC.

Each data symbol is three samples long. This results in a data block of 78 symbols per line in the unscrambled format. The symbol rate is 455 * Line Frequency, or 7.109375 MegaSymbols per second. The typical rate is 1.22 MegaSymbols per second.

The six audio channels and the clock reference burst are transmitted in what would ordinarily be the horizontal blanking period in the PAL waveform. The 11 uS is occupied by the data symbols.

Each symbol is a pair of bits in a four state modulation format. Twenty symbols are reserved for the clock reference burst. This is a two level signal and is ten cycles long. The frequency is 277.5 * Line Frequency or 4.3359375 MHz. The average level of this data determines the zero chrominance level.

Each data block consists of; 2 separation symbols, 45 symbols, 2 separation symbols, 20 clock reference burst symbols, 2 separation symbols and 6 symbols.

The audio channels are transmitted using the Dolby Deltalink system. This is the adaptive delta modulation system covered in Chapter 4. Each audio channel contributes thirteen samples and one control bit during each line period. The function of the control bit alternates with each line. The bit controls two things; the step size and the de-emphasis. Two error concealment bits and a parity bit are contained in each channel. The parity bit is used to check the six error concealment bits in each data block. A data channel is also provided for. Two bits are used for this service. The audio data rate is 204 Kb/s.

The teletext is transmitted during the vertical blanking interval. The VBI is nominally twenty five lines long. In addition to VBI test waveforms, this period contains the teletext in packets of data each 377 symbols long. Lines 9 to 13 carry the actual teletext packets. Lines 1 to 8 carry the subscriber address, the clock recovery data and the synch recovery data. The teletext is in ASCII format at a rate of forty characters per line. As the teletext service is valuable in its own right, it is encrypted.

Access Control

The access control system in the B-MAC decoder appears to be hierarchical. Each decoder has an identity which is embedded in the decoder's microcontroller. This identity is used to decrypt the authorisation data and possibly the period keys. The period keys are then used to decrypt the session key or seeds.

There is a set of period keys which each decoder must have in order to properly decrypt the session keys. In the United States, some channels change the key set every Wednesday. The period keys are stored in EEPROM but merely a set of period keys will not make the decoder operate as a pirate decoder.

The B-MAC encoder generates the encryption pattern based on a seed that can, if necessary, be changed every quarter of a second. This seed is then transmitted in an encrypted format in one of the packets in the VBI. In this respect B-MAC is similar to D2-MAC and its period key - session key - control word hierarchy.

The actual cryptographical algorithm is similar to the Data Encryption Standard algorithm. It is perhaps based in part on the DES but due to the restrictions on exporting DES equipment, it would have had to have been significantly different than the DES. Therefore since there is not enough information on the algorithm, hackers have not approached it from this angle. The hardware avenue was much easier.

B-MAC Hacks

The B-MAC system is an old system. What was secure in the mid eighties is not secure now. The technology has advanced and so have the skills and resources of the hackers.

One of the things that made the video section of B-MAC secure was that it was digitally compressed and it was in a non-standard format. The cost of video ADCs and DACs was relatively high. Therefore the reasoning was that hackers would not be able to afford to hack the video. More importantly the potential customers would not be able to afford the pirate video descramblers.

The logic was good for a finite lifetime system. Unfortunately B-MAC is not a short lifetime system. When a company uses B-MAC it is in for the duration. The cost of the decoders is relatively high and therefore to re-equip the network would be costly.

As the technology available to hackers progressed, B-MAC became a sitting target. While there was a policy of upgrading the technology, there were a lot of decoders in the field. Retrofitting these decoders would be a costly affair and most channels and services seemed to prefer to absorb the minimal piracy.

The hacks on B-MAC fall into two classes the stand alone video hack and the hook hack. Of the two the most damaging is the hook hack. So far this has only affected the 525 B-MAC decoder.

The Hook Hack

When the channels in the United States started to scramble with VideoCipher II, B-MAC also came under examination. While the hack on B-MAC was not as simple as the VideoCipher II hack, it was hacked. At first, strange messages started to appear on American hacker bulletin boards. They mentioned the Zero Power Chip which was supposed to replace a chip in the B-MAC decoder. The replacement chip was supposed to provide descrambled video and audio.

Apparently what had happened was that someone had figured out how to extract the identity from the B-MAC decoder's microcontroller. The microcontroller was supposedly secured but by some method it was possible to jam it and read the program. Scientific Atlanta had blown the read fuses. The microcontroller used in the 525 B-MAC decoders was the 68705. This is the EPROM version of the 6805 microcontroller.

Of course the decoder needed the period keys to operate properly. The keys were being stored in the 1K EEPROM, the 9346. Initially, these keys were not being changed with any great frequency. Possession of these keys alone was not enough to make the decoder operate. The decoder had to be authorised and the authorisation data may have been stored in the RAM on the microcontroller.

It is now possible to buy a 68705 reader. This piece of electronics will allow you to dump the contents of the B-MAC decoder's 68705. The cost is $2500 in US Dollars. Roughly that is IR£1500 at the current rates.

B-MAC KEYPULLER and KEYWRITER.

This portable unit will extract seed keys and rom code rom all MC68705U5S (P3's & P5's series of microprocessors). Weighing less than 2 pounds this unit is completely portable (only 8 cm. by 20 cm.) and a computer is not required. Simply remove the MC68705U5S from an authorized box and place it in the 40 pin ziff socket. Insert a ZERO POWER RAM chip into the other socket. Set the switches to the READ ONLY mode and power it up. A flashing red led will indicate the device is in the process of reading the rom code and keys from the MC68705U5S. Four minutes later when the light stops flashing the process is complete. You can verify the process by setting the switches to the VERIFY mode and both the red and green light will come on. The process is complete and correct.

The ZERO POWER RAM chip has the capacity to hold information in two banks. The top half is referred to as Bank 1 and the bottom half is Bank 2. The data that you have read into the banks can now be saved to a file by reading it with your eprom burner as a 28C64 EEPROM. You now have a binary file with 8192 bytes in it. The seed keys and rom codes are now located in this file and can be modified with a standard editor to suit your needs. An absolute clone of the original microprocessor can also be programmed.

To program a new MC68705U5S, simply set the device to the program mode. Insert the programmed ZERO POWER RAM chip into the smaller socket and then place a MC68705U5S into the 40 pin socket and select which bank in the ZERO POWER RAM chip that you want to program into the MC68705U5S. The ZERO POWER RAM chip will still have the last data in it that you read or you can program it with the binary file of your choice.

** B-MAC Keypuller = $2000.00*

FutureVision

170-3350 Fairview St., Burlington, Ontario, L7N 3L5, Canada

Call Ron On: + 1 416-572-0642

The Video Only Hack

There are rumours of the launch of a video only B-MAC decoder in the United States. Though the decoder has not been publicly demonstrated, it exists.

The weakness of the video section should be apparent. To descramble the video, a circuit to differentiate between data and video has to be built.

By using the chroma reference level between the data burst and the chroma, the line stores can be triggered. This is the key to descrambling the video. The output of this circuit can be used to gate the video into a three line store.

The video detection circuit is suggested because trying to determine the delay sequence may be difficult. As the data block is within preset limits, a window comparator could be used.

The line stores would be of different length. The first line stores would be a temporary memory for the line. The second line store would be the memory for the line being operated on. The contents of this line would be clocked into the third storage line at a slower frequency. This would digitally expand the video. The output of the third line store would then be fed to the digital to analogue video converter.

Although B-MAC is the primary system for high fee applications there seems to have been few if any hacks. The incentive to hack it is there. Some hackers are frequently offered sums of over one thousand pounds for a pirate decoder. More often than not this is for a video only decoder. There have been a few video only decoders in Europe but these were built for personal rather than commercial use.

The one thing that has worked in favour of the Racing Channel is that it is easier to go to the betting shop than to buy a decoder. In some cases, the service used by the betting shops could be rebroadcast.

Since the Racing Channel is a specialised service, the demand breakdown is different from that of a movie channel. The main demand for pirate decoders comes from those actually involved in the racing business. These people have the money to pay but were

unable to obtain the service from SIS. According to a report in one of the trade magazines, SIS are going to launch a lower cost version of their service for this part of the market.

Examining the B-MAC decoder provided some problems. In the early days of the SIS Racing Channel, the decoders were hardwired into the mains supply. If the power went down the decoder had to be reauthorised. The procedure for this involved a telephone call to the authorisation centre in the UK.

Any real examination had to be carried out when the decoder was powered up and authorised. This was the easy part. The cover was taken off the decoder. The cameras and oscilloscopes were ready. Then the photographs were taken. Unfortunately electronic flashes were used. The voltage spike was picked up by the decoder circuitry and the decoder was reset. The flashes were quickly replaced by magnesium flash bulbs and the decoder was reauthorised.

With the photographs, it was possible to start to draft a circuit diagram. Time was of the essence. The work could only be carried out when there were no punters about. The photographs were developed and the circuit diagrams were drafted. It was perhaps one of the most complex reverse engineering operations in Europe to that time.

The next stage of the operation was to source all of the components without arousing any suspicions. One of the worst mistakes that any hacker can make is to openly ask for information on a custom chip without any good backup story.

The conclusion was that the only feasible method was to dump the secured microcontroller and the EEPROM. Dumping the EEPROM was the easy part. The EEPROM IC was a 9346. This is a 1K serial EEPROM. The 256 bit version is used in mobile telephones to store the telephone's electronic serial number. A modified EPROM programmer copied this information. Unfortunately this was not enough.

Some hackers noticed that there were barcodes on the back of the decoders. It may have been that the barcodes held the identification data of each decoder. The main problem was that the identity data was held in a secured microcontroller. Unlike the 525 B-MAC version, which used the 68705, the 625 B-MAC version used the 68HC11. According to some sources Scientific Atlanta considered the Euro-

pean hacking environment to be potentially more hostile than the USA. Of course the alternative explanation was that they had just marketed a more advanced version in Europe.

The main European hacking work on B-MAC was carried out prior to the launch of ASTRA. The market was much smaller. The number of dish owners in Europe was quantified in thousands. There were some descramblers being developed for FilmNet, Premiere the English movie channel, and BBC. The scrambling systems used at that time were analogue and descramblers were easy to build. When ASTRA was launched, the ease of hacking FilmNet created the biggest market satellite pirate descramblers. At the peak of the market, at least 1.5 Million pirate FilmNet descramblers were in use in Europe.

What must be worrying Scientific Atlanta is that the European market has changed and there are some hackers who are examining the feasibility of marketing a B-MAC video only decoder.

The D-MAC Standard

The D-MAC is effectively the English MAC standard. This is primarily because it was used on the UK's first, and possibly last, high power DBS service. It can carry eight 15 KHz audio channels or their equivalent in data services.

D-MAC Specifications

Number Of Lines Per Frame: 625

Lines With Data: All

Video Lines: 24-310, 336-622

Luminance: Y in each line

Chrominance: U in odd lines, V in even lines

Interlace: 2:1 Aspect Ratio: 4:3

Luminance Compression Ratio: 3:2

Chrominance Compression Ratio: 3:1

Sampling Clock Frequency: 20.25 MHz

Instantaneous Bit Rate: 20.25 Mbits/second

Samples Per Line: 1296

Luminance Samples: 697

Chrominance Samples: 349

Bits Per Data Packet: 206 (1 Run in bit + 6 bit H synch word + 2 * 99 bits data + 1 spare bit)

Line 624: Data and analogue reference levels.

Line 625: 648 data bits

6 bits - horizontal synch word 32 bits - clock run-in

64 bits - vertical synch word 546 bits - service information

Data Structure And Format

The data packets in the D-MAC signal contain the audio and the synch words. The synch word is 6 bits long. It is transmitted as 001011 and 110100 in alternate lines. The vertical synch word is 64 bits long and is transmitted at the start of line 625.

The video scrambling system used on the D-MAC signal is double cut and rotate. There is no difference between the scrambling used on D2-MAC and that used on D-MAC. This is a system whereby the chrominance and the luminance packets are cut and rotated separately. The chrominance is cut at one of 256 points and the luminance is cut at one of 256 points.

When the video is unscrambled, there is a rough video compatibility between D-MAC and D-2MAC. This is the reason that some users of BSB D-MAC / EuroCypher receivers can lock up other MAC transmissions but fail to decode their audio.

The data on the D-MAC system in each frame amounts to 164 packets of 751 bits each. These packets break down into a header, consisting of 23 bits, a packet type, consisting of 8 bits and 720 bits of audio data or in some cases other data types.

The header breakdown is as follows; Address - 10 bits; Continuity Index - 2 Bits; and the Protection Suffix - 11 bits.

The audio channels can be high quality CD types or medium quality types. The parameters for a high quality channel are 15 KHz bandwidth and 32 KHz sampling frequency. The parameters for the medium type are 7 KHz bandwidth and a sampling frequency of 16 KHz.

The audio channels have a choice of coding types - NICAM or Linear. The NICAM is the same as that used terrestrially. (See chapter 4). This is essentially a digital compression system where each 14 bit sample is digitally compressed to 10 bits. The linear type of coding uses a 14 bit sample without compression.

The EuroCypher System

The EuroCypher system was a joint venture between General Instrument and BSB. It used a variant of the VideoCipher II scrambling system as the control architecture and D-MAC as the transmission format. The decoders consisted of two elements; the access control module and the D-MAC decoder.

The video scrambling system used on EuroCypher was double cut and rotate. The chroma packet and the luma packet were independently cut and rotated. The selection of the cut points is controlled by a PRBSG.

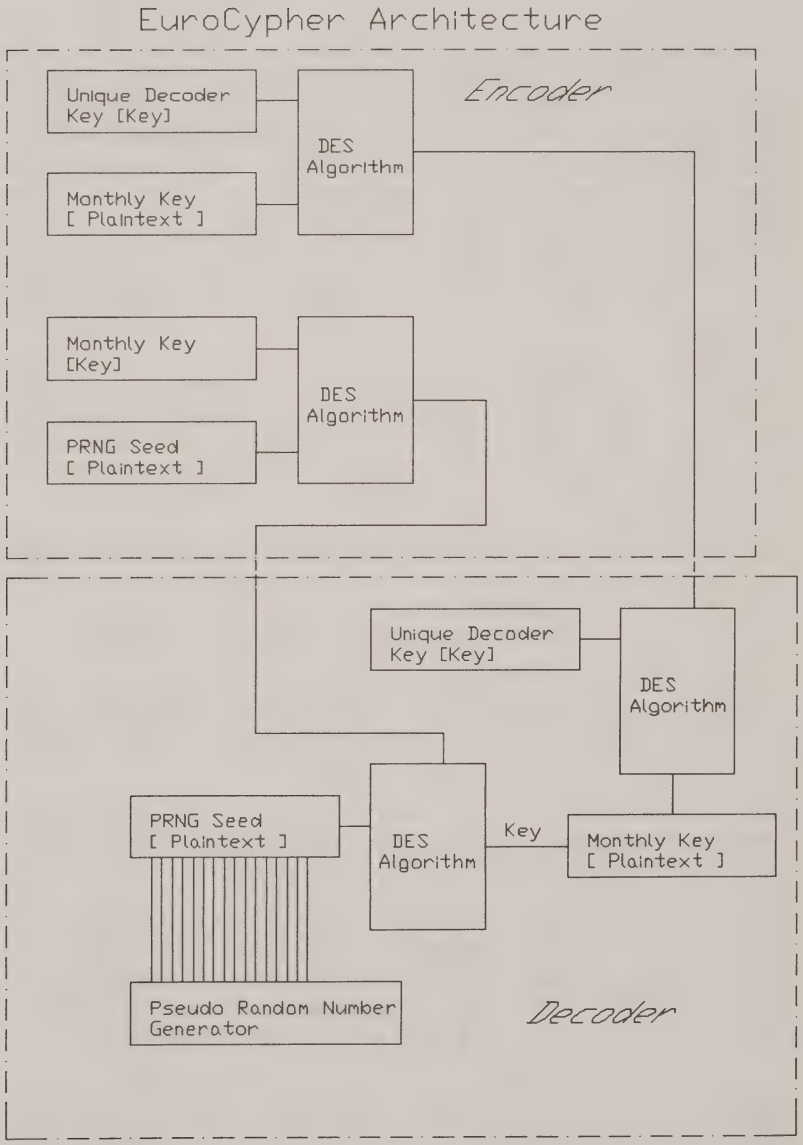
The audio on the EuroCypher system is perhaps one of the most securely encrypted types. The bitstream is EXORed with the output of a PRBSG. This PRBSG is reset every few seconds and is loaded with a new seed. The seed is sent to the receiver in an encrypted form in the addressing data.

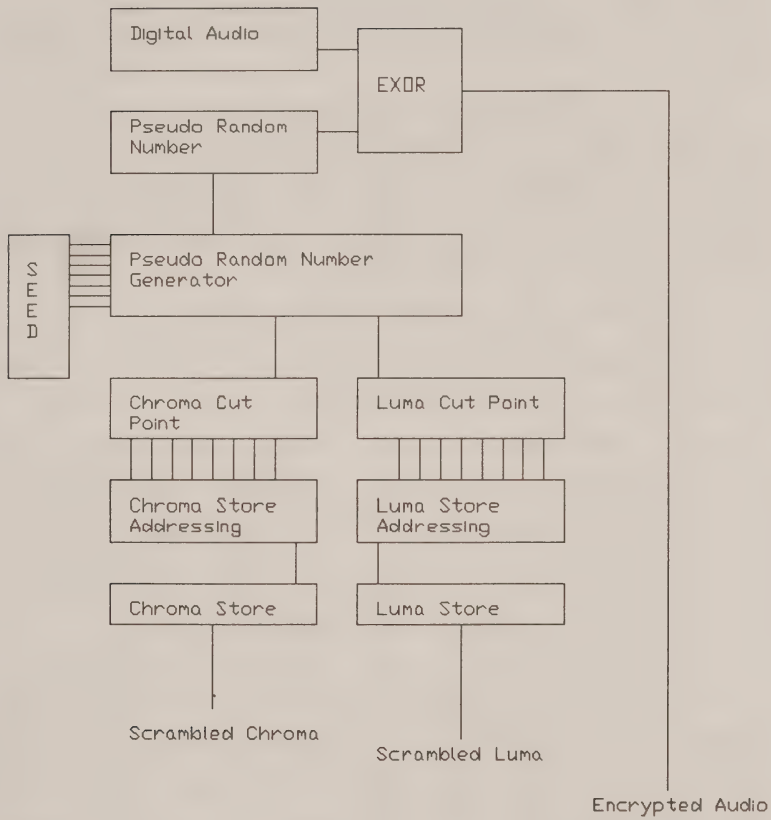
The architecture of the system is based on a receiver key - monthly key - programme key chain. The monthly key is transmitted at the beginning of every month. This key is encrypted using the DES algorithm and the receiver's unique key which is embedded in the control chips in the access control module. The receiver decrypts the monthly key and uses this monthly key to decrypt the programme key. This programme key is used to encrypt the PRBSG's seed word that is sent every few seconds.

The headend has total control over the receivers. It can deactivate receivers in real time or it can deactivate them by not transmitting the monthly keys to the receiver.

The actual EuroCypher board has a lithium battery backup to store the critical data. Apparently this information is stored in the crypto microcontroller. One of the American hacks on the VideoCipher II system used the crypto processor to external RAM link to extract the keys. It is not known if such a hack would work on this system.

During the late eighties, there was a lot of talk in the US about the research program that GI were engaged in. It was apparently to develop a chip codenamed "VSLI" or "VLSI". It was to integrate most


EuroCypher Architecture
Encoder
Unique Decoder Key [Key]
Monthly Key [Plaintext]
DES Algorithm
Monthly Key [Key]
PRNG Seed [Plaintext]
DES Algorithm
Unique Decoder Key [Key]
DES Algorithm
PRNG Seed [Plaintext]
DES Algorithm
Key
Monthly Key [Plaintext]
Pseudo Random Number Generator
Decoder



The EuroCypher Encryption Process (Simplified)

of the functions in the existing VideoCipher II decoder into a large custom IC. This actually could be the large chip in the EuroCypher decoder.

The overall on screen graphics are similar to those used on VideoCipher II. It would be no great coincidence if the core software was the same.

The EuroCypher system has not been hacked as their is no commercial basis for such a hack. Since the data flow between the access control module and the D-MAC circuitry is accessible to the hacker, it is probable that the principle of the McCormac Hack can be applied. The access control data could then be transmitted over the air to a number of EuroCypher receivers.

While this system was one that offered some security it is now a defunct system. BSkyB does not intend operating it beyond the end of 1992. It was VideoCipher's only venture of any great size on to the European stage. In more ways than one they crashed and burned.

After the BSB debacle, nobody seems to have adopted the EuroCypher system. It was considered too expensive for use on PAL based services. Many of the channels considering the system had watched the VideoCipher II situation in the United States. Generally what GI and their European subsidiary was offering was a heavily encrypted audio service in addition to a decent video scrambling system. The scrambling system was believed to be a VMS.

The VideoCipher II situation worked against GI in Europe. Nobody could bring themselves to consider the system because in the deep recesses of their mind lurked the spectre of a disaster. There would be too much of a technology transfer. Of course there would be a hacker transfer of technology as well. The hackers in Europe would have a head start on the hack. Piracy is one of the truly international fields of endeavour.

There were many factors in the downfall of BSB. Perhaps the point at which the battle between Sky and BSB was truly lost happened on a BBC "News Night" programme. Andrew Neill, one of the Sky management was in a debate with John Gau, one of the BSB management. Gau had brought along a SCART connector to show that connecting a BSB receiver to a television was easy. Neill pointed out that most of the television receivers in the UK did not have a SCART connector.

The people who selected the EuroCypher system for BSB may have operated in the best business interests. EuroCypher, to a biziod, would have seemed to be a licence to print money. Unfortunately they were crippled by the constraints of an idiotic DBS policy which dictated that the standard to be used was D-MAC and the frequency band was K-Band. The frequency aspect was decided in 1977 at the famous WARC meeting.

This policy was, as is usual with such things, ignored by the real world. Cloistered bureaucrats had decided the parameters. They were set in stone and besides they looked nice on paper. Of course technology had advanced and made the policy a moot point. ASTRA and Sky had been first. To paraphrase an American Civil War Confederate soldier: "Who ever gets there first with the most wins".

The D2-MAC Standard

The D2-MAC is effectively the European MAC standard. It can carry four 15 KHz audio channels. The primary advantage of the D2-MAC system over D-MAC is that it will fit in the bandwidth of an ordinary cablenet channel. The D2-MAC specifications are given below.

D2-MAC Specifications

Number Of Lines Per Frame: 625

Lines With Data: All

Video Lines: 24-310, 336-622

Luminance: Y in each line

Chrominance: U in odd lines, V in even lines

Interlace: 2:1

Aspect Ratio: 4:3

Luminance Compression Ratio: 3:2

Chrominance Compression Ratio: 3:1

Sampling Clock Frequency: 20.25 MHz

Instantaneous Bit Rate: 10.125 Mbits/second

Samples Per Line: 1296

Luminance Samples: 697

Chrominance Samples: 349

Bits Per Data Packet: 105 (99 bits + 6 bit h synch word)

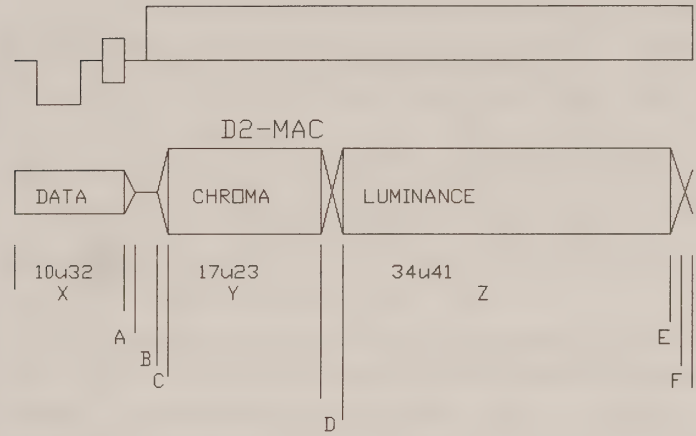
Line 624: Data and analogue reference levels.

Line 625: 648 data bits

6 bits - horizontal synch word

32 bits - clock run-in

64 bits - vertical synch word 546 bits - service information



CLOCK FREQUENCY: 20.25 MHz

X = DATA 209 CLOCK PERIODS 10.32 uS
A = TRANSITION FROM DATA 4 CLOCK PERIODS 197.53 nS
B = CLAMP PERIOD 15 CLOCK PERIODS 740.74 nS
C = WEIGHTED TRANSITION TO CHROMA 10 CLOCK PERIODS 493.82 nS
Y = CHROMA 349 CLOCK PERIODS 17.23 uS
D = WEIGHTED TRANSITION TO LUMA 5 CLOCK PERIODS 246.91 nS
Z = LUMA 697 CLOCK PERIODS 34.419 nS
E = WEIGHTED TRANSITION FROM LUMA 6 CLOCK PERIODS 296.29 nS
F = DATA TRANSITION 1 CLOCK PERIOD 49.38 nS

Video scrambling is double cut and rotate. The same system is used on D-MAC. The Audio Encryption varies. The known types are Eurocrypt M and Eurocrypt S. On D-MAC the only known type is EuroCypher.

Data Structure And Format

The data packets in the D2-MAC signal contain the audio and the synch words. The synch word is 6 bits long. It is transmitted as 001011 and 110100 in alternate lines. The vertical synch word is 64 bits long and is transmitted at the start of line 625.

The video scrambling system used on the D2-MAC signal is double cut and rotate. This is a system whereby the chrominance and the luminance packets are cut and rotated separately. The chrominance is cut at one of 256 points and the luminance is cut at one of 256 points. This type of scrambling is also employed on the D-MAC signal.

The Eurocrypt system the recommended standard for D2-MAC. There are presently two variants; Eurocrypt M and Eurocrypt S.

The Eurocrypt M variant uses an 8 bit parallel interface between the Access Control Module and the D2-MAC decoder. It also allows the use of some sophisticated functions.

The Eurocrypt S variant uses a 9600 Baud serial interface between the Access Control Module and the D2-MAC decoder circuitry.

The France Telecom Visiopass system uses a Bull PC2 Smart Card of the type described earlier. The cryptographic algorithms and control architecture are different and as such provide a stumbling block for any potential hacker. There is the probability that the McCormac Hack principle can be applied to this system. Such an attempted hack in France would be tricky for a hacker. The laws relating to piracy are draconian in France. Of course it is possible to operate such an operation outside of France.

The EuroCrypt-M System

EuroCrypt-M is the scrambling system used on the D2-MAC standard. It is one of the most widely published systems. Most of the information in this section was gleaned from the official France Telecom specification. The main part of the information necessary to hack this scrambling system was therefore freely available.

The sequence generator used for descrambling the video and audio data is a Pseudo Random Binary Sequence Generator PRBSG. The PRBSG is reset with a new seed or Control Word every 256 Frames. The frame counter is eight bits wide.

The system is based on the detachable secure processor philosophy. The smart card contains the critical information. The decoder is essentially a dumb terminal.

The basic key structure is hierarchical. In many respects it is similar to the VideoCipher II system including the fact that the encryption is based on DES. The final key is a control word that is used to seed the PRBSG.

The decoder itself is essentially dumb. It does contain the video and audio decryption circuitry but this requires the control word data from the card. Essentially, once the decoder has the control words flowing to it, it will continue to descramble the video and audio. This makes it possible to hack using the McCormac Hack.

The entitlement control and management messages flowing to the card have to be checksummed with a hash function. The hash function is resident in the card. The length of the hash is 64 bits. It is now believed that the hash function is the modified form of DES used in ECB mode.

This section is concerned with the weaknesses and hackability of the EuroCrypt system rather than the overall operation of the system. Therefore I will only concentrate on what was relevant to hack the system.

The Card And Its Data Structure

The smart card used on the EuroCrypt system is EPROM and the CPU is 6805 based. It therefore could be emulated by a microcontroller after the EPROM and ROM are dumped. The most logical method of doing this is by reverse engineering the card. Alternatively since the encryption system is so heavily reliant on the DES architecture, the necessary keys could be number crunched.

The card - decoder protocol conforms to the ISO 7816 specification concerning microprocessor based smart cards. The first version of the smart card was limited in operation. It contained 6K of ROM, 128 Bytes of RAM and 8K of EPROM.

There are two types of entities on the card; the Service Entity and the Issuer Entity.

The Service Entity

This is the data relevant to the particular channel. It contains all of the information necessary to generate the control words from the over the air data. The information in the Service Entity breaks down into the following subsets.

The Descriptor DESCR

This section contains the programme provider identifier or PPID. This is the 20 Bits that indicates that indicates the channel's identity. It also designates the types of access available, e.g. subscription, PPV, IPPV. It also includes a service lock which allows the Service Entity to be locked out.

The Keys

There are two types of keys, Management Keys and Operation Keys. The management keys are concerned with decrypting the entitlement control messages and other management data. The operation keys are used to compute the control words and are therefore the most critical.

The Label

This is merely a name for the channel, e.g. FilmNet, and is not actually used by the card for any purpose. The length of the label is 10 bytes.

The Programme Provider User Address

The PPUA is a four byte address that identifies the user in the channel's access control system. The first three bytes indicate the user's Shared Address (SA) and the other byte indicates the user's position in the Shared Address block. This byte is designated the CUSTWP. Essentially this allows the users to be accessed and controlled in blocks of 256.

The Geographical Code Address

The GCA indicates the area that the user is in. Generally the GCA is used for geographical area blackout. This is also known as the Group Customer address. It is 32 bits in length and represents an eight digit hexadecimal coded number. The first three bytes are the Geographical Code, (GC). Typically these bytes are allocated from the six most significant bits of the customer's international phone number. The other byte is the subject code, (SC).

The Entitlements

Basically this is what the card is permitted to decrypt. The information in this section is the subscription, programmes or the amount of credits available. Of course before the card proceeds to generate a control word, it will check this section to see that it is permitted.

FAC

This is the general purpose data and is not critical data. Typically it would be the telephone number of the subscription centre (for modem link back) or other data.

The Issuer Entity

The issuer entity is essentially the soul of the card. It contains the information that is common to all of the Service Entities. The information stored in this entity is in four subsets.

The Unique Address

The UA is thirty six bits wide. This is the card identification code. It is used for card management by the issuer or the programme providers.

The PIN Code

This is just like the PIN code for bank cash card machines except in this application it relates to pay services and other functions.

The Maturity Rating

This is the period for which the present card is valid. When the card is reset, this rating is one of the first items of information returned from the card.

The Preselection Area

This section is used to store pre-booked programmes and other events. The programmes stored in this area will then be accessed without the user having to select them on the day.

There are two extremely important routines that provide indications as to the characteristics of the critical data. Above all, one of them actually gives the number of keys in use on a particular service at the time the service is selected. This is an unusual attribute for a system.

Card Reset

When the card is inserted in the decoder it is reset. This starts the card decoder link but of most interest when the link is established it then returns a seven byte record. The bytes are: Component Number, Mask Number, Extension Byte 1, Extension Byte 2, Locks (Card Age), ME1 and ME2. The ME1 and ME2 bytes are the status words.

Entity Selection

In order to access a channel, the card has to select that particular Service Entity. When the entity has been successfully selected, it will return a 26 byte record.

(3 bytes) PPID

(2 bytes) Memory Allocation for Entity

(1 byte) Authorised Access Modes

(2 bytes) Memory Allocation minus Memory Used

(1 byte) Memory remaining for Entity

(16 bytes) Indices of enabled keys

Of these, the last is the most critical. It is an index of the active keys on the service. The format is a nybble represented by a hexadecimal number. Padding bytes of the value FF are used where the number of keys active is less than 16.

Eight of these keys are management keys and the other eight are the operation keys. The management keys are designated 00 to 07 and the operation keys are designated 08 to 0F.

The actual length of the keys appears to be 64 bits or eight bytes. This indicates that the crypto algorithm in use is DES or DES like.

This system is a one level system. The card is the sole security of the system. When it is hacked, the system is compromised. A new card has to be issued.

There are four elements required for the hack. The hash function, the crypto algorithms, the management keys, and the operation keys. A minimal hack requires the hash function, the crypto algorithms and the operation keys.

How EuroCrypt Was Hacked

At the moment the EuroCrypt system as used on TV1000, FilmNet, Canal Plus and Cine Cinema has been hacked. Pirate smart cards are readily available for the system.

Like the VideoCrypt hack, the origins of the EuroCrypt hack are shrouded in mystery. Some consider that the official smart card was reverse-engineered. Others suspect a leak whereas another theory is based on a cryptological reverse.

Whatever the origins, the system is now hacked and a version of the OMIGOD hack is expected in the next few months. Perhaps one of the main factors in its downfall was the reliance on the Data Encryption Standard as the core algorithm for the control word generation and hash function.

According to information received the version of the DES used in the pirate EuroCrypt smart cards has been modified for speed. The main modification has been the removal of the initial and inverse initial permutations.

While these permutations were believed to have been included in the algorithm to slow down software implementation, there now appears to have been an ulterior motive. The process of differential

cryptanalysis was known at the time of the creation of the DES. The permutations were included not as was commonly believed to slow down the software implementation of the algorithm but to hamper or at least slow down attempts at differential cryptanalysis.

The official smart card in the system runs at a relatively slow speed. This is perhaps why the control word update occurs roughly every ten seconds as opposed to two and a half seconds in VideoCrypt.

After analysing the system, the most obvious pirate smart card would be based on a 68705 type microcontroller with a RAM for the EPROM area. There would also be either a keyboard or an EPROM socket to enable the management and operation keys to be changed.

The main microcontroller EPROM would hold the ROM program from a valid card. The RAM would hold the card's EPROM area. The keyboard would allow for a rapid key update.

Of course a minimal approach could be a 6805 type microcontroller on a printed circuit board with the proper connector pad for use in a decoder.

Of course this would have left the hackers wide open to charges of copyright infringement. These would be tenuous to say the least with EuroCrypt using a modified version of a publicly specified algorithm.

The alternative was to use the PIC16C57 microcontroller. The PIC16C54 and PIC16C84 do not have sufficient memory to hold the D2-MAC program and keys. This PIC16C57 format was the initial format for the hack.

Of course there have been a few ECMs in the past year or so. Most of them have been quickly solved by the hackers. Many of the changes in keys on the FilmNet and TV1000 cards have not affected the pirate cards. In fact it is believed that there is a common table of keys between TV3, TV1000 and FilmNet. Most of the cards on the market have these keys programmed into them. When the channel changes the key pointer then the better pirate cards follow.

Canal Plus and Cine Cinema have a larger potential key block. As a direct result of this any ECM on these channels can take slightly longer to hack. Of course with the actual high speed of the DES algorithm when implemented in hardware, a Brute Force Attack

(trying all possible keys) using a number of processors operating in parallel does tend to reduce the security of the system. This is the basis for the latest hack on EuroCrypt.

The Virtual Key Cruncher

A EuroCrypt channel changes its key. The pirate cards stop working. Now imagine a network of thousands of processors all trying each potential key.

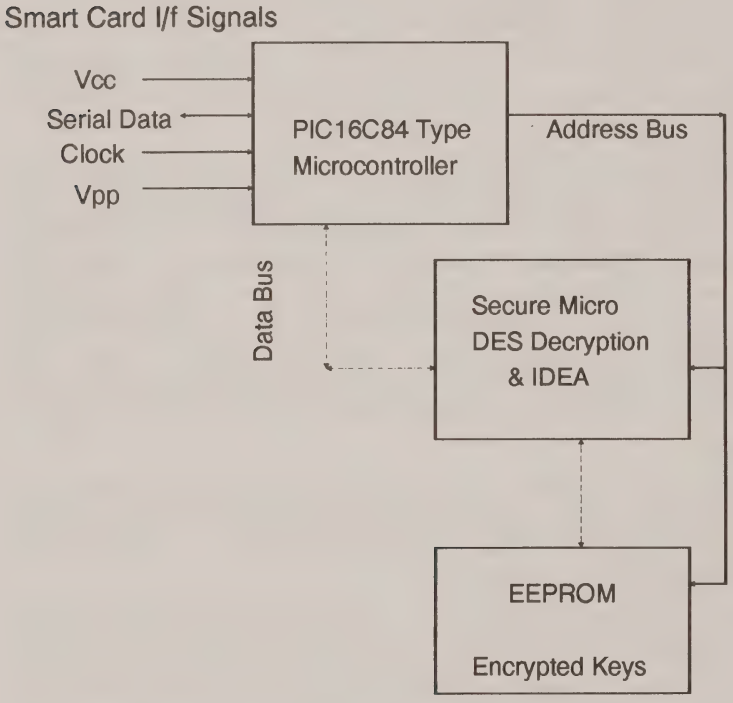
This is the latest format of the hack on EuroCrypt. The new pirate cards will use three chips. Two microcontrollers and an EEPROM. One microcontroller will contain the card interfacing and housekeeping routines. The other microcontroller, a more secure chip than has been used to date, will contain the decryption algorithm and the keydata decryption algorithm, (believed to be IDEA). This secure chip will take the encrypted keydata from the EEPROM and after decrypting it will use it in the modified DES algorithm to generate the control word which is fed via the housekeeper microcontroller to the decoder.

The obvious advantage is that the pirate card is now much easier to upgrade as the key data will only work with that particular card design. Therefore it can be distributed via BBSes or FTP or even printed on faxes or magazines.

The update facility is only one of the innovations in this hack. The main one is that each pirate card becomes part of a virtual computer network when the user is finished watching for the night. He just leaves it in the decoder on the channel that has changed keys. If he comes down in the morning and the card is decoding the channel then he returns the card to the manufacturer for a prize of five thousand pounds or so.

Each pirate card tests a range of keys on the channel. With one microcontroller, the process of finding a key by a Brute Force Attack would take a very very long time. With a virtual network of a few thousand cards this search time may well be reduced to days.

The EuroCrypt Virtual Key Cruncher



The other control lines are not shown in this diagram. The Secure Microcontroller handles the decryption of the control word and also the decryption of the actual keys.

The keys are stored in an encrypted format in the EEPROM. This allows a control over the cards by the hackers in a fashion hitherto unseen. It also means that the pirate cards can be personalised on a dealer basis so that key updates can be distributed on a dealer basis rather than the present blanket update basis.

Perhaps the most important aspect of this card design is that it is reusable unlike many of the PIC16C57 designs on the market at present.

***** Warning *****

Under the Irish Broadcast Act 1990, it is illegal to operate MMDS receivers on an MMDS net without the permission of the net owner. It is an offence to manufacture, sell or install pirate cable or MMDS descramblers or MMDS receivers.

The fines under the 1990 Broadcasting Act are significant. The first offence of pirating a signal whether on cable or MMDS is punishable by a fine of up to £1000 and or a few months in prison. Distributing pirate decoders or any form of organised piracy is punishable by a fine of up to £20000 and a possible two years in prison.

In the UK, piracy of or interference with cablenet signals is an offence under various laws.

In most European countries, there is tough legislation on the statute books for dealing with cable piracy. Due to the localised nature of a cablenet, the chances of a hacker being caught are high. If the company doesn't actually know about the hacker, there is always the likelihood that some nasty neighbour will inform the cable company.

Clearly, I am not advocating that the reader should use this information to defraud a cable or MMDS company. This information is for educational purposes. If you do decide to misuse this information, consider this question; how do you know that your cable or MMDS operator hasn't read a copy of this book and therefore is ready for what you may do?

The MMDS section of this book fills a market gap. There are no decent books on MMDS available in Ireland. This section will provide an insight into what has been happening. It also contains some representative circuits and antennas. The circuits and antennas have been published previously. It should be useful in third level colleges. Most of the books on microwave engineering are either too theoretical or are too out of date.

8: Cable And Microwave Distribution

This chapter is in two sections. The second section covers microwave television as applied to the Irish situation. The system chosen for use in Ireland is based on the Canadian 2.5 GHz system. The UK appears to be in favour of going with a 12 GHz system. Frankly this is is presently impractical. It is difficult to predict if microwave television will be adopted throughout Europe. Should a system be adopted then it will likely be a 2.5 GHz based system.

Microwave television is a natural progression of cable television. In the US it is known by the paradoxical term "Wireless Cable". The large cable companies will be offered first choice of the franchises. This is to protect the investments and jobs of those working in the cablenets.

Most of the advocates of MMDS for all areas are, in general, ignorant of the financial and technical problems involved. Many of them see an MMDS operation as a long term operation where financial breakeven is reached three years after startup. The reality is that breakeven has to be reached within the first year and a half at most. MMDS will succeed in the hinterlands of the cities. The failure risk in the less populated areas will be higher. Effectively MMDS is another stage in the evolution of the cable nets.

Cable television seems to have passed by the UK. Most of the other countries in Europe have healthy cablenet operations. It is often a source of great amazement to the English tourist in Ireland that the average Irish city has upwards of eleven television channels. The introduction of scrambling on various cablenets has provided some cable hackers with easy targets.

Section 1: Cable Scrambling Systems

Many of the satellite television scrambling systems started out as cable television scrambling systems. This chapter deals with the techniques used in cable television scrambling systems and the techniques used by the cable system hacker. The techniques used can be every bit as complicated as some of the best satellite systems.

The best analogy to illustrate the difference between the space hacker and the cable system hacker is that of the bomber pilot and the foot soldier. The space hacker, like the bomber pilot rarely sees those affected by his actions. The cable system hacker,

like the foot soldier can see the people affected by his actions. There is a common factor in all these cases - professional isolation. The liberal minded would call it something else.

Notch Filters

The simplest technique used by cable companies to deter non-paying users is the simple notch filter. A notch filter is placed on the user's line so that he or she cannot receive a particular channel. This requires a control box for every few houses passed. As long as the control box is secure, there is very little that the average non-paying user can do. Any interference with either the main signal carrying cable or the cable of a paying user will easily be detected. This technique was used extensively in the United States until more secure systems were developed. The average non-paying user did not pose a problem to the cable companies, the cable system hacker was the real problem.

The favourite hack was to place a piece of coaxial cable along the main signal cable. One end of the coaxial cable was then connected to a wideband amplifier. In most housing estates, the main signal cable is fed along the sides of the houses. This makes it extremely easy to conceal the "pirate" coaxial cable.

This technique is widely used by electronic technicians, engineers and television engineers. Another hack depended on the depth of the notch. A tuned amplifier with enough gain was merely inserted in the line. It worked with the earlier LC notch filters. The advent of more secure or deeper notch filters defeated this hack.

Legally the cable companies found it difficult to deter the indirect tap described earlier. Since there was no direct connection to the cable company's property, it was difficult to prove theft of signal. Since the signal emitted from the cable was not really meant to be emitted it would have been embarrassing for the cable company to sue someone for capitalising on the inferior quality of their gear. The simplest and commonest solution to the hack was to encase the cable with a metal pipe.

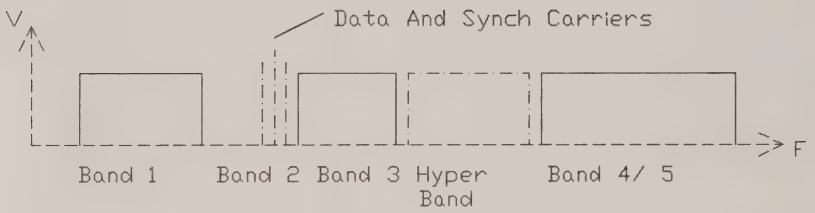
Plain Jane

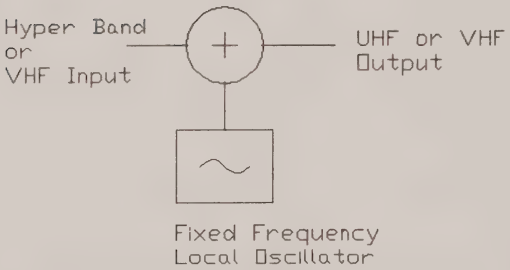
The next system to see use was the "Plain Jane" system. This was not really a scrambling system. It was merely frequency shifting. The television channels were frequency shifted to a block outside the bandwidth of the normal television tuner. In the early eighties, there were a number of companies trying to sell VHF based systems in the UK. The majority of UK televisions only had UHF tuners and therefore would not have been able to pick up VHF. Virtually anybody who could solder could have hacked their system.

Some of the Plain Jane systems used the frequency block in between VHF Band 3 and UHF Band 4. This was quickly defeated not only by the hackers but by the television manufacturers. They used tuners that could cover these frequencies and advertised their sets as being "cable ready". One idiot of a marketing executive actually named this frequency block "S-Band". This caused some confusion with some satellite television experimenters who thought that the tuner could cover the industrial satellite IF block.

The Plain Jane system is not widely used at present and only an idiot of a system manager would choose such a system. With the advent of more television channels, some cablenets in Ireland are licensed to use the frequency block between Band III and Band IV. To date the only transmissions have been descrambler tests and channel tests.

Plain Jane





The Plain Jane system is rarely used as it offers extremely limited security. Many cablenets are permitted to operate channels in the Hyper Band but these channels if used will generally be test channels or scrambled channels.

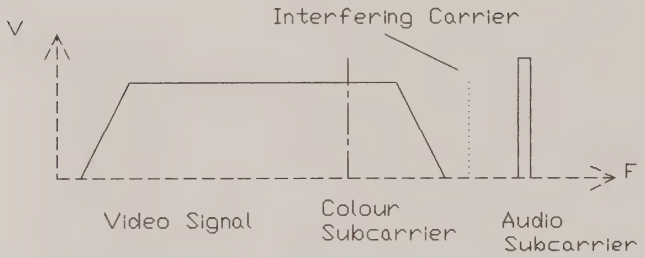
Interfering Carrier

The interfering carrier is a low security system that is more suited to cable television applications than to satellite television. The interfering carrier can be applied the signal IF or at baseband. It is generally situated in an area of low video activity. The level of the interfering carrier is the key its effectiveness. When the level of the interfering carrier is close to that of white level, severe interference will result. All that is required to remove the carrier is a simple high Q filter tuned to the frequency of the carrier.

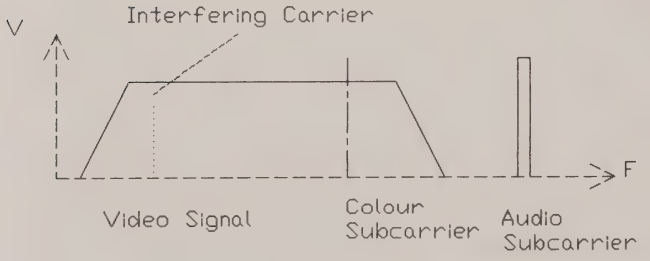
There are two methods that are used to improve the security of the system; multiple carriers and varying frequency carrier. From a hacker's point of view, the multiple carrier version is the easier of the two to defeat. The official descrambler would use a switched surface acoustic wave filter, (SAWF), to notch out the interfering carriers. The notching or switching sequence would be controlled either by addressing or by a programmable read only memory IC, (PROM), in the official descrambler. The filtering in the hacker descrambler would be carried out using standard LC circuits. The quality may not be as good as the official descrambler but it does produce a watchable picture.

The variable frequency carrier is more secure and will deter the "Sunday Driver" hacker but is not secure against a real hacker. In this system a carrier of constantly varying frequency is injected into the baseband. The multiples of the line frequency are the commonest centre frequencies for these carriers. The commonest technique used to hack this system is the tracking filter. Such a descrambler is difficult to construct as it requires a lot of adjustments before it will operate properly. The "Sunday Driver" hacker will not generally have the expertise or the test equipment necessary to develop a descrambler. Unfortunately for the cable system owners life is not so simple. The real hackers will eventually sell the descrambler designs to the "Sunday Driver" hackers.

Interfering Carrier Scrambling



Interfering carrier scrambling applied at baseband level. The carrier is placed between the video and audio signals in the baseband spectrum. A simple notch filter can remove it.



In this variation, the interfering carrier is placed in the video signal. This makes it harder to remove. It is essentially the RF method. The interfering carrier is added and removed when the signal is at the IF stage rather than at baseband. Surface Acoustic Wave Filters are used for this process. The SAWFs can be fabricated with a very narrow stop band.

Synch Suppression

The technique of synch suppression is widely used as a cable scrambling technique. The two commonest are sine wave synch suppression and pulse synch suppression. Both of these techniques have been mentioned in the satellite television scrambling chapters but they will be examined in detail here.

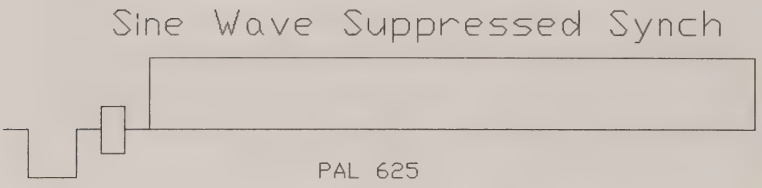
It should be stated that synch suppression scrambling is not permitted in some European countries. Synch suppression is an antiquated form of scrambling that can easily be overcome. A cable company that chooses this type of scrambling would be taking a severe risk. Most of the pirate FilmNet descramblers could be modified to operate on a synch suppression system other than a sine wave type.

Sine Wave Synch Suppression

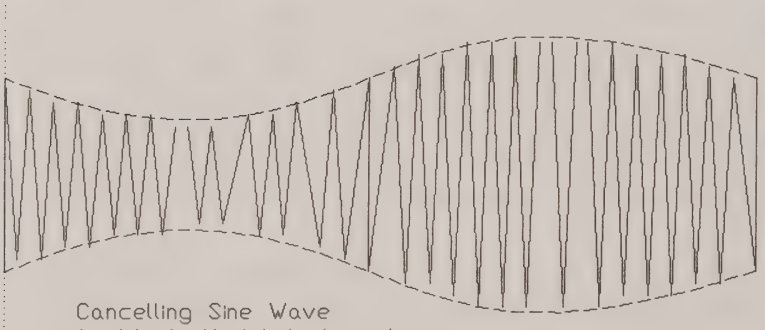
Sine wave synch suppression is ideally suited to cable television scrambling. It can either be applied to the signal at baseband or to the transmitter amplifier. The transmission mode for terrestrial television is amplitude modulation. (For the purists - Vestigial Sideband.) This means that the sine wave cannot be removed from the demodulated signal by a clamp in the way that the dispersal waveform is removed from the video of a satellite broadcast.

The frequency of the sine wave can either be line frequency or a multiple of the line frequency. The wave is phased so that it pushes the line synch pulse up in to the video region of the signal. (Note: Positive going video and negative going synch waveform used for example.) With some systems, the sine wave is switched off during the vertical blanking interval. This causes the frame to lock on the television but there is no line lock. To complicate matters further, the video can be inverted and or reduced in amplitude. The reduced amplitude option is rarely used due to the complications that it can cause.

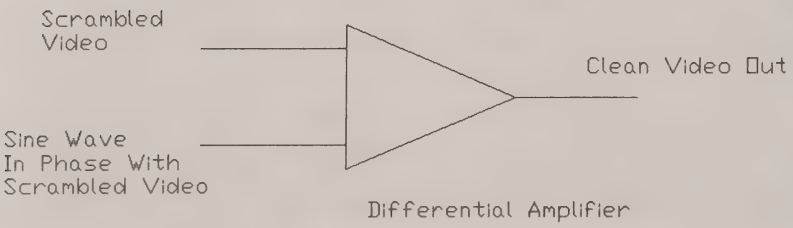
There a number of ways to descramble such a signal. The official decoders generally use a sine wave transmitted on either the audio subcarrier or a separate subcarrier. The actual sine wave is amplitude modulated on to the FM carrier. The level of the sine wave on the audio subcarrier is very low so it is affected by any



Sine Wave Synch Suppression



Cancelling Sine Wave
Amplitude Modulated on to
FM audio subcarrier.



Differential Amplifier

limiting circuit in the television receiver. The separate subcarrier can be near to the channel or it can be in a totally different band. It is the more secure of the two.

The methods used by hackers to defeat the sine wave technique are in some respects far simpler than those used in the official descramblers. The following paragraphs detail the procedure used for hacking such a system.

1. The video is the first thing to be examined in the procedure. Examining the video on an oscilloscope will give the approximate frequency of the sine wave. This information is essential for the next stage. The video signal used in the examination is raw baseband from the video demodulator rather than the video output of the VCR or television.

2. The raw FM audio subcarrier is then fed to the oscilloscope. This test will determine if the system uses a separate subcarrier for the decoding signal. This audio subcarrier must not be FM limited as the descrambling waveform is often amplitude modulated on to the FM subcarrier.

3. If no sine wave is present on the audio, a scanner is used to see if there is a separate subcarrier. Most cable system hackers use a home brew spectrum analyser made from a tuner-IF strip with modified AGC time constant instead of a scanner.

4. If steps two and three prove negative, the interfering sine wave has to be stripped from the video and antiphased for cancellation. The frequency of the interfering sine wave will be higher than that of the line frequency. The official descrambler would not use filtering to remove a line frequency sine wave though there are probably exceptions. An official descrambler would use a phase locked loop to descramble the signal. This method is a very costly and very effective method of descrambling. A typical hacker design would use a high Q filter and adder for cancellation. Such a circuit can be made for a few pounds. This kind of circuit was used to hack the SAT-TEL SAVE system used on the BBC-KTAS link on the Intelsat at 27.5 degrees West. In this case, the interfering sine wave was in the region of six times the line frequency.

5. If the sine wave is present on the audio it must be stripped off with a filter. Alternatively, if the sine wave is present on a separate subcarrier it must be demodulated and filtered. The

separate subcarrier could be very close to the channel and so it may be present if the IF output of a tuner tuned to the scrambled channel. In this case, an FM demodulator would be used to demodulate it. With some systems, an amplitude modulated subcarrier is used.

6. One of two methods is used to descramble the video signal; baseband antiphasing or RF antiphasing. RF antiphasing involves feeding an antiphased sine wave to the AGC pin of the tuner. The IF output of the tuner is then upconverted to VHF or UHF. This technique is popular with American cable system hackers. European hackers tend to favour the baseband antiphasing technique. This technique involves combining an antiphased sine wave with the video. A modulator can then be used to bring the video and audio back up to UHF if required. The SCART or Euroconnector means that the modulator is not needed for most of the recent European televisions. Antiphasing without a phase locking circuit produces a distorted video with very messy chrominance. The synch pulses can also be affected. This causes line tearing on video with a high white concentration.

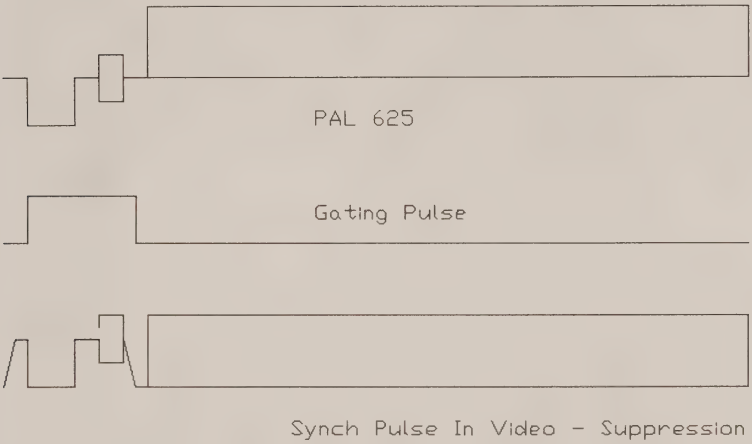
Pulse Synch Suppression

Pulse synch suppression is a more complicated scrambling system than the sine wave synch suppression system. It primarily interferes with the line synch pulses by pushing them into the video region of the signal. There is another similar technique, (synch attenuation), that is often confused with pulse synch suppression.

Pulse synch attenuation is where the magnitude of the synch pulse is attenuated. Pulse synch suppression is where the magnitude of the synch remains constant but the maximum and minimum levels of the pulse are interfered with. The system is also known as gated synch suppression. Essentially it is gated level shifting.

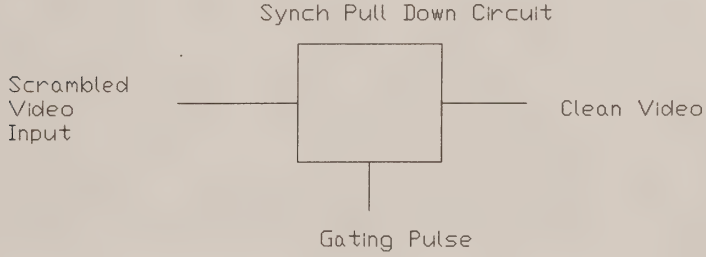
The two systems are used by cable companies. The gated attenuation is easier to apply to an AM signal and as such it is the older of the two systems and the more common. The gating pulse can be applied to the IF automatic gain control, AGC, line on the IF amplifier at the headend. To descramble the signal, an inverted gating signal is applied to the AGC line of a tuner. The reference signal is often transmitted on the audio at a very low level in the

Pulse Synch Suppression



Synch Pulse In Video - Suppression

This system is primarily a baseband system rather than an RF system. This means it would require a separately controlled AGC on the IF strip.



same way as the reference for the sine wave synch suppression. A separate subcarrier can also be used. This system is easier to hack at RF than at baseband though some commercial designs have probably used a baseband approach.

Pulse synch suppression rules out the use of comparators for resynching. As was mentioned earlier, the synch pulse is pushed into the video region and a comparator would be triggered by the video information. A series of monostables triggered by the reference signal is generally used to resynch the video. Again the same options are open to the system designers. This is more of a baseband system than an RF system and it is this fact that gives the system an added level of security.

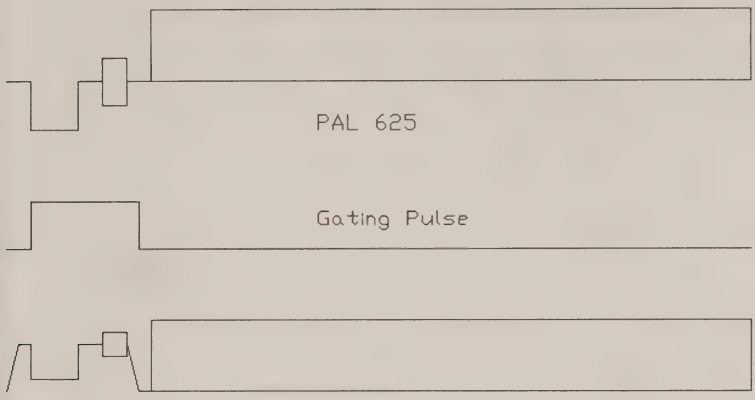
Pulse Synch Attenuation

Pulse attenuation can be applied to the whole horizontal blanking interval so that it also attenuates the colour burst as well as the horizontal synch pulse. This kind of system will generally have more than one attenuation factor for security. Common attenuation values are 0 dB, 6 dB and 10 dB. Such a system pseudo-randomly switches between any of these factors. The sequence can either be stored in the descrambler or transmitted in encrypted form on the signal. The reference signal is usually transmitted in one of the ways mentioned earlier.

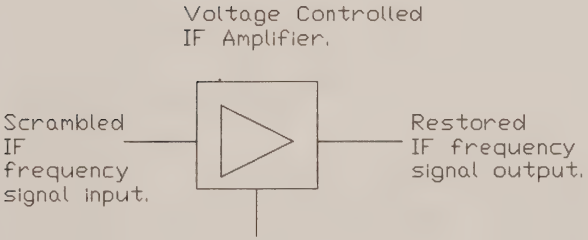
On one of these synch attenuation systems, the algorithm for the attenuation sequence is contained in the descrambler. The descrambler identity is held in a RAM. A lithium battery is placed across the RAM. This RAM also holds the validation details of the descrambler. The case of the descrambler was adorned with the usual theft of signal is a crime stickers and anti-tamper screws. The anti-tamper screws were obviously designed by someone who had never seen a pair of cutters commonly used in electronics. The blades of the cutters fitted the slots in the screws thus enabling their extraction.

In some of these variable synch attenuation systems all the random attenuation is for naught. A weak resynching carrier is transmitted on the audio. The hack for this is extremely simple. This resynching carrier is stripped off the audio carrier using a stereo demodulator IC such as an MC1310 or LM1800. Both of these ICs use a PLL. The VCO, which would be locked to the 15.625 KHz

Pulse Synch Attenuation



Synch pulse and colour burst are attenuated and as a result are pushed into the video region of the line. The Vertical blanking is not generally attenuated. The reason for this is that the descrambler derives its AGC from the vertical blanking.



The voltage controlled IF amplifier has 0 dB gain when the pulse gating signal is low. This low state occurs during the active video region and the vertical blanking. During the time when the pulse gating is high, the amplifier has a gain of 3 dB or 6 dB depending on the system in use.

carrier would then be phased with the scrambled video using a 4528. The new synch pulse would be gated in using a 4066, as the old attenuated synch pulse would have to be removed from the waveform. The stereo indicator facilities on the ICs would be used to switch the PLL in and out of circuit thus enabling operation on scrambled and clear signals. In cases where the colour burst is included in the attenuation, the monostable would control a gated amplifier.

Tri-Mode Pulse Synch Attenuation

In the US and some European countries, Jerrold's Tri-Mode Synch Attenuation System is used. Though the system was developed and patented by Jerrold, other manufacturers use this system's scrambling and access control system under licence. This has given rise to the term "multi vendor compatibility". This means that a Jerrold descrambler can be used, with the proper authorisation codes on a cablenet that employs the Scientific Atlanta Tri-Mode system.

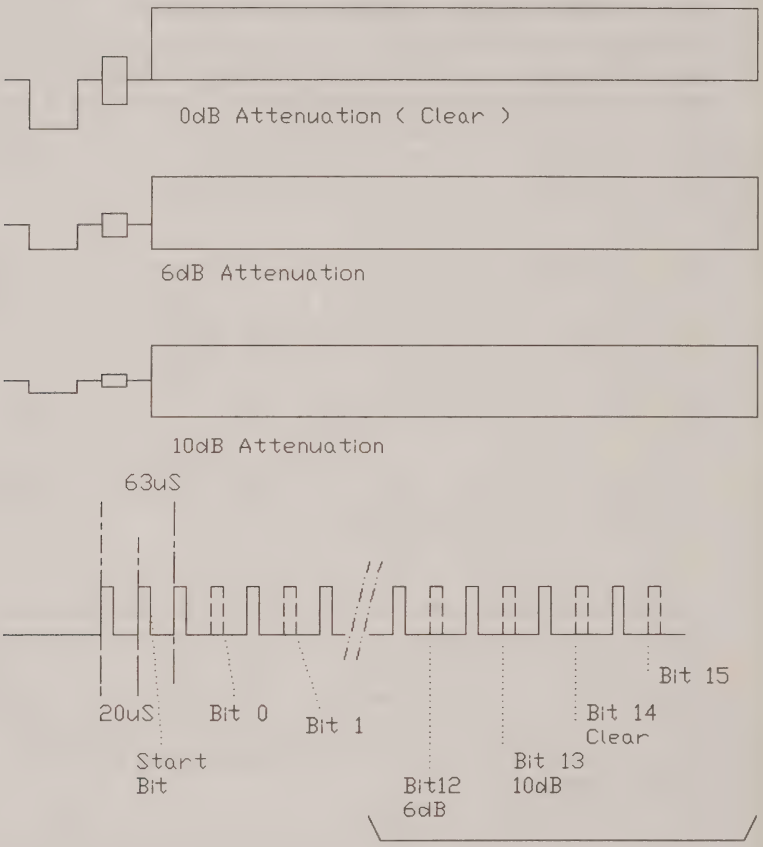
The tri-mode pulse attenuation method of scrambling is one of the standard methods used in the US and Europe. It is often billed as being highly secure. The reality is that the method is far from secure and articles on how to hack it have been widely published in the US. Radio Electronics published a complete design along with printed circuit board layout for this system. Luckily for the system owners in Europe, very few cable hackers have read the American article.

The system relies on attenuating the horizontal blanking section of the line by 0dB, 6dB or 10dB. In the 0dB mode there is no attenuation and the picture is effectively clear.

The synch carrier is amplitude modulated on to the FM audio carrier. In addition to the synch information, the carrier includes data that indicates the attenuation mode in use. The information here has been synthesised from a number of American sources. Before the manufacturers of this system start whinging that I am divulging top secret information, I should say that the main source of information was the article in Radio Electronics. Therefore this information is from openly published sources.

In the NTSC system, the first 20 lines or so of each field are unused. The tri-mode system uses these lines positions to carry data. The data is carried on the synch carrier rather than the data. The data is a 17 bit packet. Each bit of the packet is inserted in the video space in the synch train. In the NTSC system, the data bit starts 20 uS after the rising edge of the synch pulse. Bits 0 to 8 carry the programme authorisation data. Bits 8 to 15 carry the descrambler enable codes. The bits 12 to 15 carry the scrambling codes. The 0dB code is 0010. The 6dB code is 1000. The 10dB code is 0100. The states of these four bits are continually changing. This is a security measure that has been reasonably successful.

Tri Mode Synch Attenuation



These four bits determine the scrambling state in use.

0010 = 0dB
1000 = 6dB
0100 = 10 dB

The scrambling mode used is that prior to a 1111 flag.

The key to the system is the detection of the state when all bits 12 to 15 are logic 1. This is the identifier. The state prior to this state is the scrambling mode in use. This hack requires sequential and combinational logic to execute.

The descrambler for this system is RF rather than baseband orientated. When a signal is demodulated it is clamped. Since the television receiver uses the blanking levels for clamping it is obvious that the result will be an unmitigated mess. The approach used in the official and the hacker descramblers is to demodulate the data and the synch carrier and use gated RF amplifiers to descramble the RF. The descrambled data would then be fed to the television receiver.

The system is an antique and is not very popular in Europe as it is not transparent in the way Cryptovision and VideoCrypt are. Both of these systems can be accessed via the SCART connector on the television. The main factor that appears to have limited the piracy on the system when it was used in Europe is the cost of the RF section involved.

To actually descramble the signal, a cable tuner with an standard TV IF output has to be constructed. Using a standard wideband tuner this would cost about £30.00. The descrambler section must then be constructed for a cost of about £30.00. The total cost for the hacker descrambler would approach one hundred pounds or so.

One rumour from a cablenet where a tri-mode scrambling system was used reflected a serious lack of security on the part of the system owner. The reason why there was no piracy was that there were no pirate descramblers only modified official ones. When subscriptions had expired, the cable company had not repossessed the descramblers. Someone had figured out how to hot wire the descramblers.

When datavoyaging in the USA and Canada, I have seen the EPROM programs posted on Bulletin Board Systems to hack the tri-mode system. It is an old system. The manufacturers may be continually upgrading its security but there are many superior systems on the market.

Synch Removal

Resynching a signal with a transmitted reference signal is easy, but what happens if no reference signal is transmitted either with the audio or on a separate subcarrier? Such a system is slightly more secure than the basic pulse synch suppression system. It is not as secure as the publicity brochures would have us believe. It will only deter the "gifted amateurs" that only exist in the minds of marketing executives. Another rule of magic can be applied here to hack this system:- "Believe what you see not what you think you see."

Most of these systems leave the first few synch pulses in each frame alone. In some cases, the vertical blanking interval test signals, (VITS), are untouched. The more secure systems only leave two or three lines untouched. The method used to descramble these systems should be apparent by now to any television engineer. The majority of commercial descramblers use an oscillator that is only locked for the few untouched lines and free running for the rest of the frame. An alternative method is the use of the long and short pulses in the frame or vertical blanking to reset a read only memory, (ROM), containing a set of data that produces a correctly timed set of gating pulses. This method is used in commercial descramblers where alternate frame inversion is an option. The odd and even frames can be identified from the frame blanking. Most hackers will use a variation of an integrated circuit television synch section to descramble this system. The ROM approach will only be used by the more experienced hackers.

Video inversion was once used as a method of scrambling. It was crude and effective. Today, dynamic video inversion is used by a number of systems. With this mode of scrambling a random selection of lines or groups of lines in each frame can be inverted. The use of video inversion on cable systems is not appreciated by cable engineers. It is too easy for the system to suffer from line tilt and other complications.

All the previous methods have one thing in common, they all can be accessed without the control of the cable company. This makes them insecure and potentially financially fatal for the cable company involved.

All good cable scrambling systems have three common characteristics which are as follows:

1. To provide any real financial security for the cable company, the set top descrambler has to be addressable. It must be possible to switch off the descrambler from the cable company office.

2. To provide any real hacker security it must have a facility that is very difficult or extremely expensive to hack.

3. Some input from the customer such as a password or passnumber is required. Without this input, the descrambler should not work. This will curtail the use of stolen descramblers and give customers a parental lock out facility.

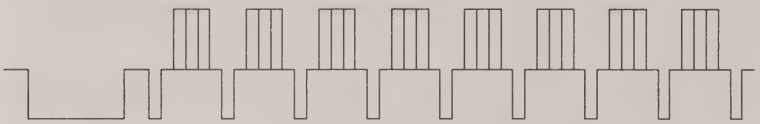
Addressing

There are a number of ways of addressing a descrambler the two commonest are In Signal Addressing and Out Of Band Addressing.

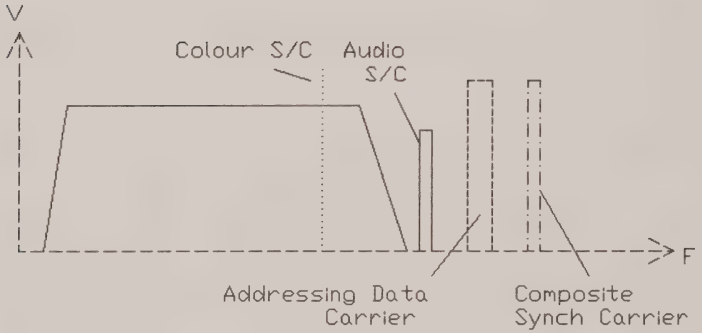
In Signal Addressing is the most complex and the most secure of the two systems. Address of the descrambler to be enabled is transmitted in the vertical blanking interval or on one of the non-video lines. The majority of addressable systems use the VBI for addressing and authorisation level and use the non-video lines for the descrambling algorithm. If the actual descrambling algorithm is stored in the descrambler then the variable data will be transmitted in the non-video lines. This method is often used with pseudo-random line inversion systems.

Out Of Band addressing is rarely used alone. With this system the addressing data and the authorisation data is transmitted on a carrier outside either the bandwidth of the signal or the band of channels. These carriers can easily be detected by a spectrum scan. They are more expensive as they require a separate receiver strip in the descrambler. There are probably a few cable company executives that believe that an addressable scrambling system will solve the problem of hackers or "signal pirates" as they would call them. These cable company executives are more of a risk to their companies than any hacker. The majority of the addressable scrambling systems use standard methods of scrambling the signal. These systems can easily be hacked. Even if there

Addressing - In Band

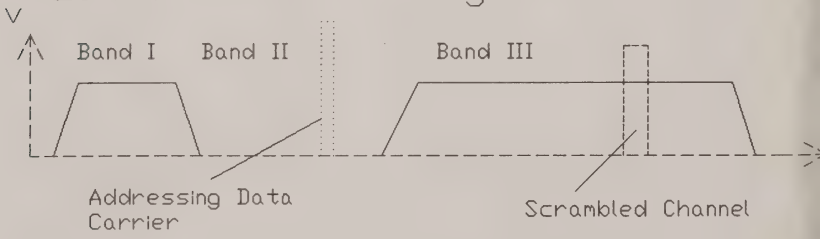


Addressing data transmitted in Non Video lines of field. This method is used VideoCrypt and Discret.



Addressing Data Carried On Subcarrier In Channel Bandwidth. This type of addressing is used by FilmNet on satellite transmissions.

Out Band Addressing



are a number of methods of scrambling, such as in the FilmNet system, they still will be hacked.

The majority of the American scrambling systems use FM'd audio technique. The next most commonly used technique is spectrum inversion. Both of these techniques date from the seventies. Virtually every recent system uses digital audio.

In the United States, Videocipher II is becoming the standard satellite and cable scrambling system. Oak ORION is also widely used in the United States. They both use digital audio. In the Videocipher II system the audio is encrypted using the Data Encryption Standard. The Oak ORION system uses a different method of encryption for the audio. There is little doubt that General Instrument will try to have Videocipher accepted as the European scrambling standard. They claimed that their system was invincible because it used the DES for encrypting the audio. The hackers made a laughing stock of them by hacking their system. Potential European purchasers of their system will now consider other options. Without being biased, there are a number of better European scrambling systems on the market. The European systems are designed with PAL in mind rather than NTSC.

Section 2: Microwave Television

The Multichannel Multipoint Distribution System, (MMDS), otherwise known as microwave television, has been adopted by the Irish Department of Communications as a means to distribute television channels in areas that would be uneconomical to cable. As was expected, the big cable companies are to be considered first in line for area licenses. This is because the MMDS system will be a threat to them.

The legitimate cable companies have made a considerable investment in their cablenets. With respect to the size of its population, Ireland is one of the most cabled countries in Europe. In the UK cable television has met with sporadic success. In Ireland, all the major cities are cabled. Eventhough the subscribers may sometimes complain about the quality of the service they depend on the cablenet to supply their television viewing. If an MMDS transmitter service commenced within ten or twenty miles of the cablenet, some of the subscribers would purchase MMDS reception equipment. Depending on the proximity of the transmitter, a considerable percentage of the cablenet subscribers would opt for the MMDS. This would put the cablenet's financial future in danger and more importantly, it would put the jobs of the people working for the cablenet in danger. It is for this reason that the cablenets will be offered the first chance at the areas surrounding their cablenets.

With satellite television, the state monopoly has been smashed and the captive audience of RTE has disappeared. People in the areas as yet uncabled seem to want a choice of stations. The pirate rebeam operators are taking the English television channels and filling this market gap. MMDS is intended to eliminate these pirates and to introduce some sort of order into the broadcast situation.

The system that is being introduced in Ireland is based on the Canadian system. There was a letter published in a provincial newspaper from a rebeam pirate claiming that the Canadian system did not work. The letter also claimed that the system could not be implemented in Ireland. This pirate had no known experience of either the Canadian system or microwave communications. The letter was of the type to be expected from a rebeam pirate.

It is interesting to note that the rebeam pirate who wrote the letter is still actively involved in rebeam operations. He is also very active in selling ASTRA satellite television systems. He also claimed that he was providing a service for the good of the community. This excuse is a common one among these rebeam pirates who, in most cases, are only concerned with their own financial good.

Full MMDS coverage of Ireland or any country cannot be achieved. While many areas will cover up to 75% of the franchise there will still be a need for fill-in stations. The most feasible type of fill-in station would be a short distance link to a communal antenna feeding a small cable system. This kind of system would place most of the engineering on ground familiar to the people who work for the cable companies. Microwave technicians and engineers would be required for the microwave work as it would be safe to say that the majority of people working for the cablenets have had little or no microwave experience.

The frequency range for the new microwave television system will be 2.5 GHz to 2.68 GHz. This frequency allocation differs from the American version. The American frequency range is from 2.15 GHz to 2.16 GHz and from 2.5 GHz to 2.68 GHz.

The basic concept of the system is that each subscriber will have a rooftop antenna and microwave converter. The required channels will be transmitted from a MMDS transmission installation. Each receiving antenna will have to have a clear line-of-sight view of the transmitting antenna. Microwave signals are drastically attenuated by any obstructions such as trees, buildings and hills.

One of the main attractions of the MMDS system is the small amount of power required to cover an area. It has been estimated that approximately one watt of RF power is required to give a mile of usable signal area. This implies that 100 miles could be covered using 100 Watts. This is a theoretical situation. In reality the areas are much smaller, typically the area being thirty or forty miles in diameter. This makes the prospect of direct substitution of the pirate rebeam operations more feasible. The main problem that the cable companies have with the pirates is the uncontrollable reception of the pirated signal. With microwaves, the creation of reception black spots is a lot easier than at UHF though in some cases their creation is totally non-intentional.

The band is divided into odd and even channels. Odd channels are designated Group A and even channels are designated Group B. Each franchise is allocated odd or even channels. This ensures that there is a gap of 8 MHz between each channel on an MMDS net.

Group A

Channel	Frequency Limits	Vision Carrier	Sound Carrier
1	2500 - 2508	2501.25	2507.25
3	2516 - 2524	2517.25	2523.25
5	2532 - 2540	2533.25	2539.25
7	2548 - 2556	2549.25	2555.25
9	2564 - 2572	2565.25	2571.25
11	2580 - 2588	2581.25	2587.25
13	2596 - 2604	2597.25	2603.25
15	2612 - 2620	2613.25	2619.25
17	2628 - 2636	2629.25	2635.25
19	2644 - 2652	2645.25	2651.25
21	2660 - 2668	2331.25	2667.25

All frequencies are in MHz.

An offset of 7.8125 KHz is permitted in some cases. This is to reduce the possibility of interference from other nets. The nets with offset frequencies are designated A+ and B+.

The use of odd and even channels also opens the possibility of direct downconversion to bands where existing RTE transmitters are operating. The channels could theoretically coexist on the band with minimal interference. This would be a theoretical rather than practical possibility.

Group B

Channel	Frequency Limits	Vision Carrier	Sound Carrier
2	2508 - 2516	2509.25	2515.25
4	2524 - 2532	2517.25	2531.25
6	2540 - 2548	2533.25	2547.25
8	2556 - 2564	2549.25	2563.25
10	2572 - 2580	2565.25	2579.25
12	2588 - 2596	2581.25	2595.25
14	2604 - 2612	2597.25	2611.25
16	2620 - 2628	2613.25	2627.25
18	2636 - 2644	2629.25	2643.25
20	2652 - 2660	2645.25	2659.25
22	2668 - 2676	2331.25	2675.25

All frequencies are in MHz.

The concept of MMDS is to supply a number of installations via an omnidirectional transmitting antenna. The franchises are defined by a transmission radius.

The transmitting equipment will be standard MMDS transmission equipment. The frequency tolerance will be +/- 500 Hz. This tolerance can easily be achieved by use of a crystal oven. The transmitters will be synthesised to maintain this tolerance over all channels on a net.

The minimum signal level at the edge of the franchise is 45dB. The maximum effective isotropic radiated power allowed for this performance is 32 dBW. The EIRP is the transmitter output multiplied by the antenna gain. The antenna gain in this case is referred to an isotropic radiator. An isotropic radiator is a point in space that radiates equally in all directions.

The height of the transmitting antenna is calculated by measuring its height above the average ground level between three and fifteen kilometres distance from the antenna. This procedure is carried out for eighteen radials. The starting radial is at true North and the angular distance between each radial is twenty degrees. The effective height of the antenna is the worst value obtained from this procedure.

The field strength at the edge of the franchise is not supposed to exceed 66dBuV/M. The EIRP of the transmitter will be adjusted to achieve this value. In order to avoid interference to other nets, the maximum antenna height for full power transmissions is two hundred metres. The EIRP will have to be reduced by 1 dB for every twenty five metres up to a maximum of 5 dB at the maximum height of three hundred and twenty five metres.

The reception specifications for the system detail a 6 dB noise figure for the receiver. This figure is easily achieved using GaAsFETs. A noise figure of 4 dB could be reached by using some of the cheaper silicon high frequency transistors.

The output impedance of the receiver is to be 75R in order to match the input impedance of the television. The permitted output blocks are as follows.

Band I 47 MHz - 68 MHz 21 MHz Block

Band III 174 MHz - 230 MHz 56 MHz Block

Band IV / V 470 MHz - 862 MHz 392 MHz Block

In the official receivers, no overlap of local RTE transmitters is allowed. A bypass circuit to allow the subscriber to switch between MMDS channels and off-air channels has to be provided in the design. The official receiver also has to comply with the electrical safety regulations. The RF output level has to be 60 dBuV with a tolerance of +12 dB or -6 dB.

The receiver specification is generous. The noise figure specification can easily be reached by a number of techniques. The output blocks may provide a problem. For the lower blocks, the receiver will have to have a variable local oscillator. This adds to the

overall cost of the receiver. The UHF block provides the most promise as the full MMDS block can be block downconverted to UHF.

The antenna specification is similarly generous. The recommended gain of the receiving antenna is 22 dBi with a front to back ratio of 20 dB. The orthogonal polarisation discrimination on the main lobe is 19dB. The diameter of a parabolic antenna with this gain at 2500 MHz and with an efficiency of 55% is 64.84 centimetres.

The following list is a list of the proposed MMDS transmission sites in Ireland. The actual transmission sites will probably be different as these sites may cause problems due to either visibility or current usage.

Proposed MMDS Transmission Sites

Number	Location	Range	Block	Polarisation
1	Buncranal	20	A	Horizontal
2	Dunglow	15	B	Horizontal
3	Dunkineely	15	A+	Vertical
4	Ballycroy	20	A	Horizontal
5	Foxford	20	A+	Vertical
6	Sligo	15	B	Horizontal
7	Stradone	15	A+	Vertical
8	Cavanagarvan	10	B	Horizontal
9	Dundalk	20	A	Horizontal
10	Curraghroe	30	A	Horizontal
11	Mullingar	15	B+	Vertical
12	Navan	20	B	Horizontal
13	Galway	30	B	Horizontal
14	Cloghan	20	A+	Vertical
15	Kildare	20	A	Horizontal
16	Howth	20	A+	Vertical
17	Wicklow	15	B	Horizontal
18	Ballybunnion	20	A+	Vertical
19	Limerick	30	A	Horizontal
20	Boggan	30	B	Horizontal
21	Nurney	15	A+	Vertical
22	Gorey	10	B+	Vertical
23	Kilcotty	15	A	Horizontal

23a	Ballycanew	20	A	Horizontal
24	Farranfore	15	B	Horizontal
25	Mallow	20	A+	Vertical
26	Villierstown	15	A	Horizontal
27	Cheekpoint	20	B+	Vertical
28	Drinagh	15	A	Horizontal
29	Cork Airport	20	B	Horizontal

All ranges are in miles.

There will be certain areas in these franchises where reception will not be possible. If these areas are large enough, a separate fill-in net may be established. The AH+, BH+, AV and BV are not used in the initial MMDS plan. These combinations are reserved for the second stage of the plan. It is possible that the fill-in stations will use these combinations.

Many companies in Ireland have not yet scrambled their signals. If and when these companies are let loose on microwave, they may still be transmitting the signal in the clear. If this occurs, they are risking being undermined by hackers. The Irish Broadcasting Act 1990 clearly makes piracy a crime. If you wish to experiment get permission. Hacking MMDS is not the same as satellite hacking. The risks are too great. This may sound like heresy but part of being a good hacker is knowing when to hack.

The cable companies in Ireland are relatively new to the field of microwave engineering. Most of the present hackers have been involved in satellite television from the early days. In the early days, the only band worth experimenting with was C-Band. The cost of microwave integrated circuits from the United States was too high for most. The alternative was to use "home brew" converters and amplifiers. The Antiparallel Diode Mixer and the 3 dB Hybrid Mixer were two of the commonest designs used by the experimenters. These designs were built using microstrip etched on standard G-10 fibreglass board. The advantage of the antiparallel diode mixer was that the local oscillator frequency was half that which would have been required by a standard mixer.

In order to have a tunable IF block, the C-Band Block was converted down to UHF, (470 to 870 MHz). This did not cover the full C-Band block and as a result the microwave oscillator had to be retuned depending on the section of the block required. A standard UHF tuner was then used to tune this converted block.

As can be seen from the hacker downconverters, the whole system is financially insecure. The actual cost of the hacker converter is in the region of ten pounds. The cost of the microwave antenna would be approximately the same. The cable companies will probably have to charge a fee in the region of two to three hundred pounds per annum. A commercial pirate design could be manufactured and sold for about one hundred and fifty pounds. This would destabilise the cable companies and microwave companies who have not scrambled their signal.

In some areas, cable companies hired non-technical people to do their installations. Some of these people are probably still employed though in an indirect manner. There are many microwave antenna designs that can be used for MMDS. These people will have to be trained in antenna identification and detection. It will be virtually be impossible for the MMDS operators to check out every house in their area.

Lumped Microstrip Components

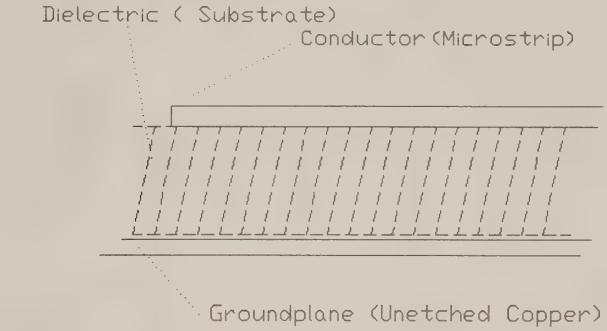
The concept of an MMDS receiver system is not very different from the C-Band downconverter. The MMDS block has to be downconverted to UHF for use by a UHF tuner. No further processing is required as the transmission format is AM VSB. This means that the downconverted MMDS signal can be used by an ordinary television unless the signal is scrambled.

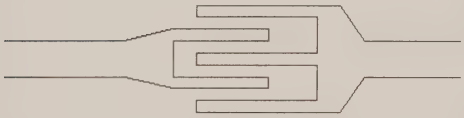
Most of the circuits at MMDS frequencies use microstrip components instead of discrete components. Microstrip is a circuit element in which the properties of a piece of printed circuit board track are used to simulate a discrete component. This a cheaper option as the value of the component can be controlled through the manufacturing process. The value of the component does not change drastically from board to board.

A piece of printed circuit board track on a double sided printed circuit board, with one side acting as a ground plane,

Microstrip Components

Microstrip Cross Section

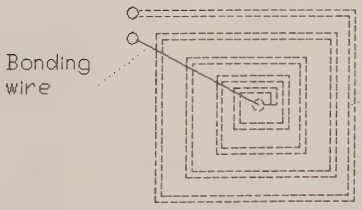




Interdigitated Capacitor.

The interdigitated capacitor is formed from two pieces of microstrip track. The value of such capacitors is typically below 10pF.

Squared Spiral Inductor



The track impedance is typically above 120R.

operating at a given frequency has resistance, inductance and capacitance. It also has a frequency dependent property of impedance. The inductance of the piece of track is mainly affected by the thickness of the conductor, the width of the conductor and the length of the conductor. The capacitance of the track is mainly affected by the thickness of the printed circuit board material and the area of the conductor.

By using the properties of a piece of track, passive components can be fabricated. Individual capacitors can be formed by interdigitating two pieces of track. The ends of each piece of track are shaped like fingers so that they interlock but do not touch. The gaps between each finger or digit provide a repeatable amount of capacitance. The value of the capacitance is usually in the region of fractions of a picofarad. It is an easy way out when there is no conventional component that can be used. The commonest applications are matching networks and filters.

Inductors can also be easily and repeatably fabricated. In their simplest form they are fabricated from thin tracks. The tracks can be spiraled to increase the inductance achievable in a given area. When drafting inductors in microstrip, it is easier to draw lines than spirals. The spirals are "squared" to make then easier to draw or plot. The squared spiral also provides more inductance per area than the spiral.

While it is easy to use a CAD package that will do the calculations and plot the boards, many of the top hackers prefer to draft the boards by hand. The rationale behind this is simple. Any fresh faced university graduate can use a CAD package but only a real designer can do it by mind. A well designed microstrip board is a work of art and the essence of art lies in the mind rather than in the brush.

The Antiparallel Diode Mixer

The antiparallel diode mixer has the unconventional characteristic of requiring a local oscillator running at half the normal frequency.

The mixer consists of two microstrip resonators and two Schottky barrier diodes. With reference to the diagram, A is an open circuited half wavelength line at the signal frequency. The intermediate frequency is taken from the midpoint of this line. The other line is a short circuited quarter wavelength at the normal oscillator frequency.

The oscillator level required for this mixer is 0 dBmV. The isolation between the RF port and the local oscillator port is good. The mixer does require some preamplification prior to the mixer and some filtering after the mixer.

This design was used in many of the commercial C-Band downconverters in the US. It is very easy to fabricate and as such this should make it popular with hackers. It is used as part of the second hacker downconverter detailed later in the chapter.

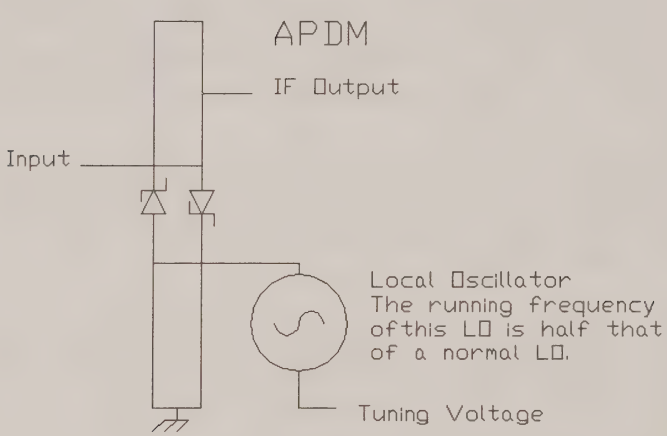
The Ratrace or 3 dB Hybrid Mixer

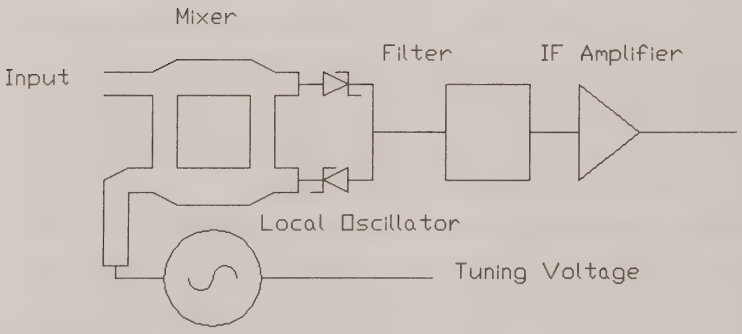
The ratrace mixer is essentially a balanced mixer. By counting the number of quarter wavelength phase shifts in each signal path it can be seen that the signal and local oscillator waves arrive at each diode in antiphase with each other. The signal power and the local oscillator power are coupled to the mixer diodes with low loss. This makes the mixer more sensitive and less lossy.

The mixer is wideband and as a result it requires some form of filtering on the output. The minimum filter is a quarter wavelength open circuited stub. The stub length is a quarter wavelength at the signal frequency and as such attenuates any microwave signals at the output of the mixer. Ideally a low pass filter for the required output passband should be designed.

The noise figure of the mixer is relatively low. Figures of 4 dB to 7 dB have been quoted for C-Band. The loss of the mixer is in the region of 6 dB to 9 dB. The noise figure of the mixer is not as critical as the noise figure of the preamplifier. In this case, the signal levels require some amplification prior to mixing.

Microstrip Mixer Circuits





3dB Hybrid Mixer

The Image Rejection Mixer

When the intermediate frequency is low, the converter is more prone to interference from the image frequency signals. The standard IF of most of the first and second generation C-Band satellite television receivers was 70 MHz. This meant that the image frequency response was 140 MHz away from the signal frequency. The image frequency was within the C-Band block. The image rejection filter was a clever use of phase shifts to cancel the image frequency components.

The incoming signal was split and phase shifted by 90 degrees in the first 3 dB coupler. The two signals were then fed to two ratrace mixers. These mixers were fed from the same oscillator. The outputs from the two ratrace mixers were then combined and the out of phase components canceled.

While this design has been popular with C-Band users, its use in the United States by MMDS hackers has been limited. This is due to the relatively large PCB area required. Most designs are based on the standard G10 fibreglass board. This has a dielectric constant of 4.7 to 5. A reduction in size could be achieved by using a board with a higher dielectric constant. The problem is that the cost of the board material also increases.

The MMDS system as it stands is totally insecure. The ease with which it can be hacked must give some of the MMDS operators nightmares. To hack this system, the hacker has to convert the block in use down to UHF or VHF. Researchers have obtained usable bandwidths of 50% of the centre frequency from the 3 dB Hybrid mixer. This would make it a good choice for use in a downconverter. A local oscillator for the Irish system would be running at a frequency of about 2.0 GHz. This would convert the block down to UHF tuner range. A simple one transistor fixed frequency oscillator could be used to provide the conversion oscillator.

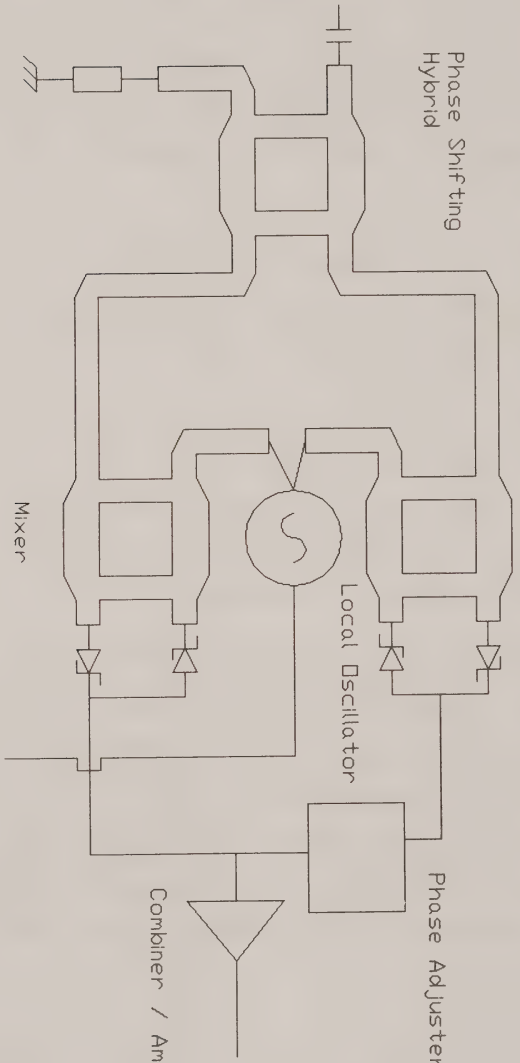


Image Rejection Mixer

The Hacker MMDS Downconverter 1

This section, as they say, is included purely for informational purposes only. The author and the publishers accept no responsibility for the use or misuse of the information by the reader.

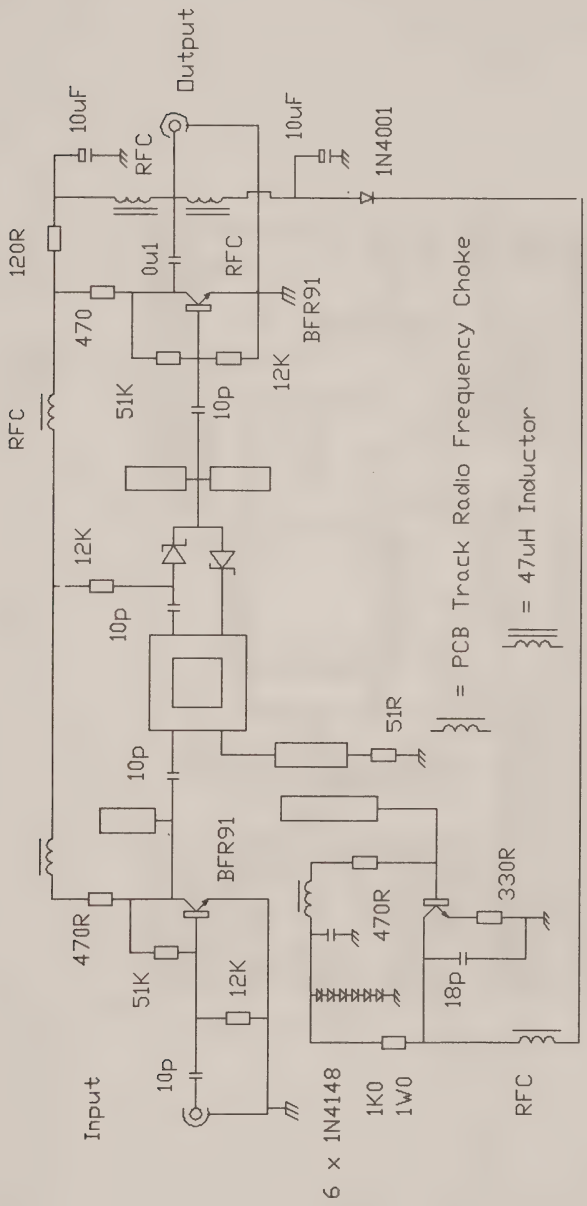
This design is based on an American design of 1982 vintage. It is a single downconversion type with its output on US Channel 3, (61.25 MHz). The components used in the design are readily available. The original design used the MRF901 transistor. The BFR90, BFR91, BFR34A transistors can be substituted for this transistor. The BFR91 would be a better choice for the oscillator transistor as it has a higher current handling capacity.

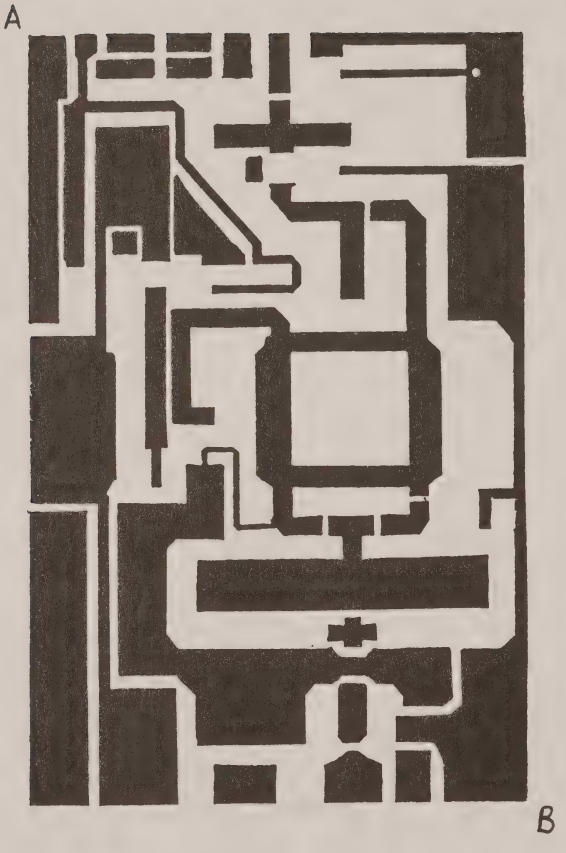
The preamplifier amplifies the incoming MMDS signal to a usable level. By using stubs, some filtering of the input is carried out prior to mixing. The BFR90 can be replaced with a microwave transistor if you are willing to do some experimenting. The increase in quality is sometimes worth the cost.

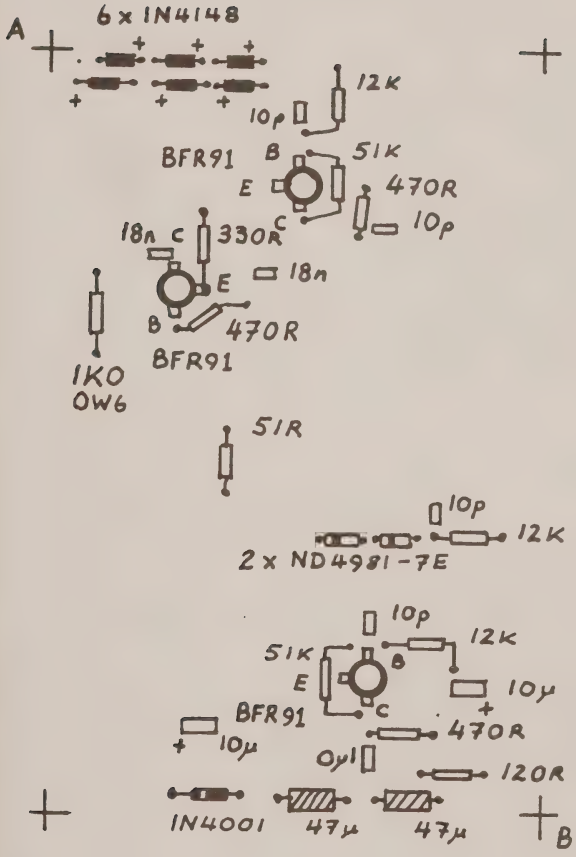
The mixer is the standard 3 db hybrid mixer. The 3 db hybrid mixer is essentially a balanced mixer. By counting the number of quarter wavelength phase shifts in each signal path it can be seen that the signal and local oscillator waves arrive at each diode in antiphase with each other. The signal power and the local oscillator power are coupled to the mixer diodes with low loss. This makes the mixer more sensitive and less lossy. The diodes are biased on to provide greater sensitivity. The output of the mixer has a wide low impedance stub to act as a lowpass filter. The filtered intermediate frequency is then fed to the output amplifier. The output amplifier is wideband. A UHF band filter and amplifier could be used at this point instead of the output amplifier.

The oscillator output is taken from the base of the oscillator transistor. The oscillator output is fed to the mixer by use of a directional coupler. The amount of oscillator power reaching the mixer is controlled by the distance between the microstrip tracks on the board. The end of the input track to the mixer is taken to ground by a 51R resistor. This is to balance the ports of the mixer. For temperature stability, a diode chain is included in the oscillator. The drift factor of the local oscillator is approximately 0.17 MHz per degree Centigrade.

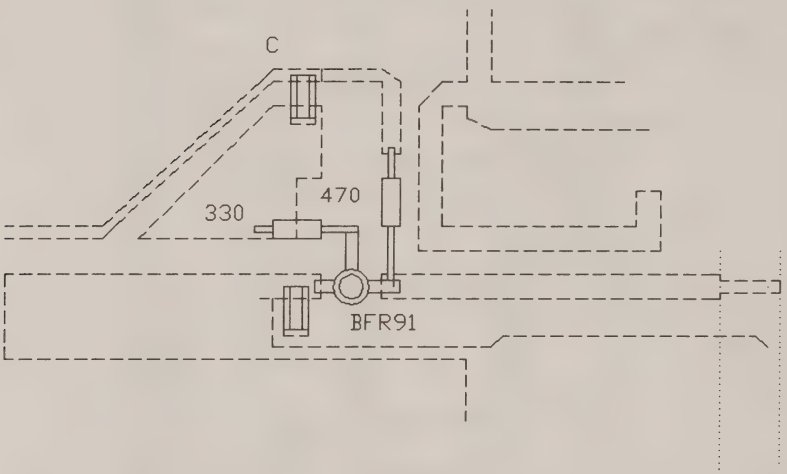
The operating range of the local oscillator is set by trimming the base line of the oscillator transistor with the supply voltage set to 14 Volts. The supply range can be varied over the 12V to 16V range.


Hacker MMDS Converter 1
= 47uH Inductor
= PCB Track Radio Frequency Choke
Input
Output
RFC
120R
10uF
1N4001
470
51K
12K
10p
0u1
BFR91
470R
330R
18p
51R
1K0
1W0
6 x 1N4148


A
B


A
6 x IN4148
12K
10p
BFR91
B
51K
E
470R
C
10p
18n
C
330R
E
18n
B
470R
BFR91
1K0
0W6
51R
10p
12K
2 x ND4981-7E
10p
51K
12K
E
B
C
10µ
BFR91
10µ
470R
0µ1
120R
IN4001
47µ
47µ
B

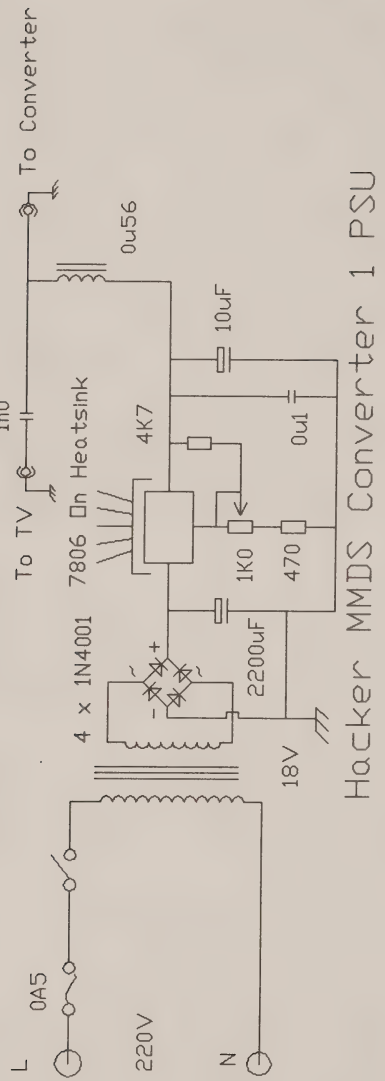
Hacker MMDS Converter 1
Local Oscillator Tuning



Trim base line for correct local oscillator frequency.

During Tuning Procedure Vcc = 14 Volts.

In the event of cutting the base line too short, the local oscillator frequency will be too high. If this is the case use the same technique employed in the tuning of Hacker Converter 2 local oscillator.


To Converter
0u56
10uF
1n0
To TV
7806 On Heatsink
4K7
0u1
1K0
470
4 x 1N4001
2200uF
18V
0A5
220V
L
N
Hacker MMDS Converter 1 PSU
Ensure that TV socket is isolated.

The previous circuit reflects the technology of the early eighties. The BFR90 transistor in the front end is noisy. A better design would use a GaAsFET amplifier. The mixer in this design is wideband. This is perhaps one area that could be optimised. The optimisation would involve the design of a microstrip filter to make the mixer selective.

The oscillator is not the most stable of oscillators. the main modification that would be necessary here would be some form of AFC using a prescaler and low frequency PLL. The oscillator signal would have to amplified in order to drive the prescaler. There are many magazine designs that can be adapted for this application.

The MMDS frequency block is near to that of a satellite television receiver IF. A satellite television tuner could be salvaged from a junked receiver. The Mitsumi types would be ideal for this experiment as they have an output centred at 479 MHz. This is in the UHF region. To downconvert the highest MMDS frequency to 1700 MHz would require a local oscillator running at 980 MHz. A stable oscillator at this frequency is easier to fabricate than a stable microwave oscillator.

The Hacker MMDS Downconverter 2

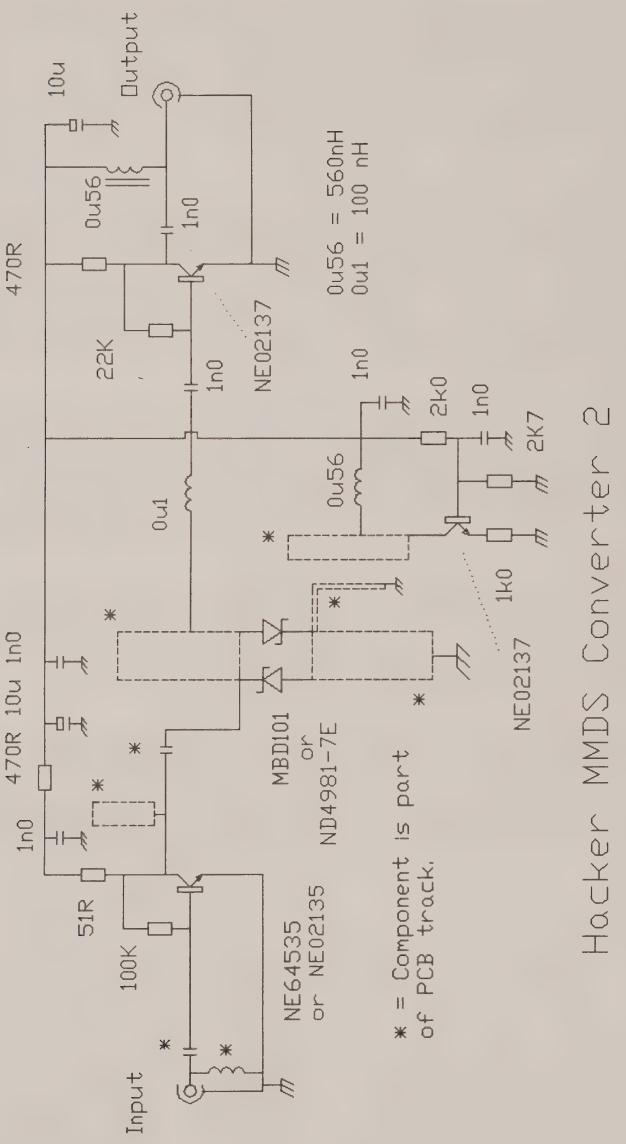
This design originally appeared in the Pink And Brown Book. The Pink And Brown Book was published in May 1986. The design had its origins in 2300 MHz amateur radio equipment. The power supply as published was a biohazard as the fuse was in the wrong position. This fault has been corrected in the version presented here.

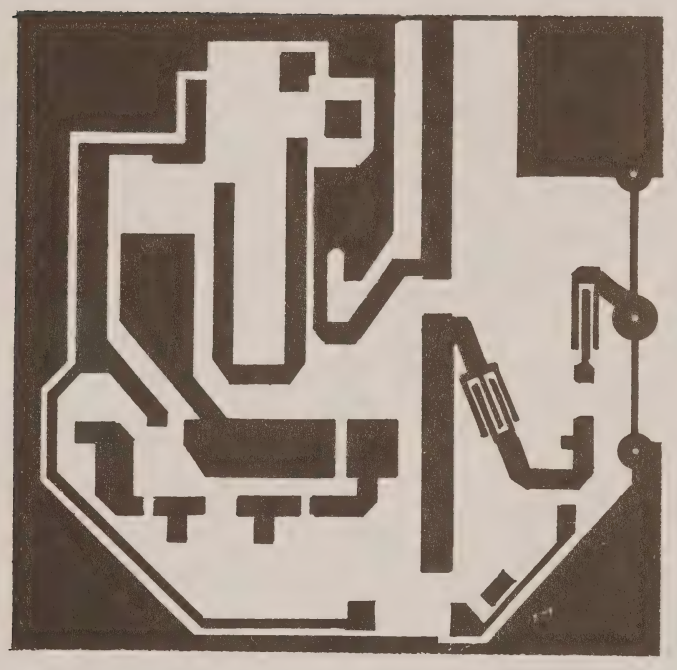
The input to the downconverter is DC shorted via two high impedance stubs which are earthed. A microstrip interdigitated capacitor is used to decouple the input of the microwave amplifier. A stub is used to tune the output of the microwave amplifier. The output of the amplifier is fed to the mixer via another microstrip interdigitated capacitor.

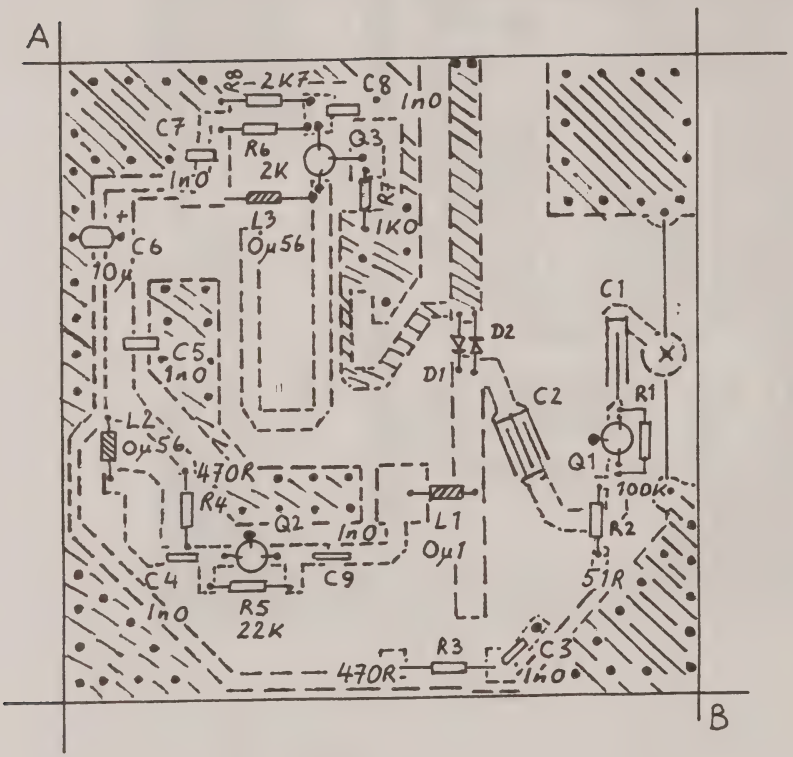
The mixer used in this design is an Antiparallel Diode Mixer. This allows the local oscillator to run at half the normal local oscillator frequency. The oscillator frequency is doubled in the mixer. The diodes used in the mixer are Schottky microwave diodes.

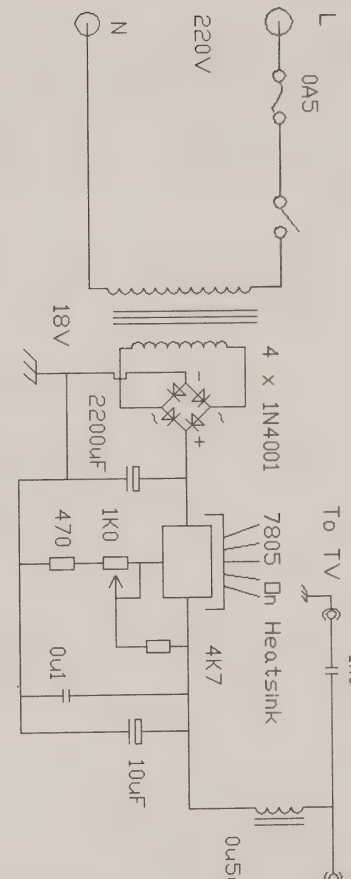
The local oscillator is a simple one transistor design. A coarse adjustment of the oscillator frequency is performed by trimming the collector microstrip element. Channel selection is performed by varying the supply voltage between 6V0 and 14V.

The output of the mixer is fed to a wideband amplifier. In the original design, the output frequency was 55 to 85 MHz. This is Band I and as such it is suitable for input to a VHF tuner strip. This would provide a baseband output for use with pirate descramblers.

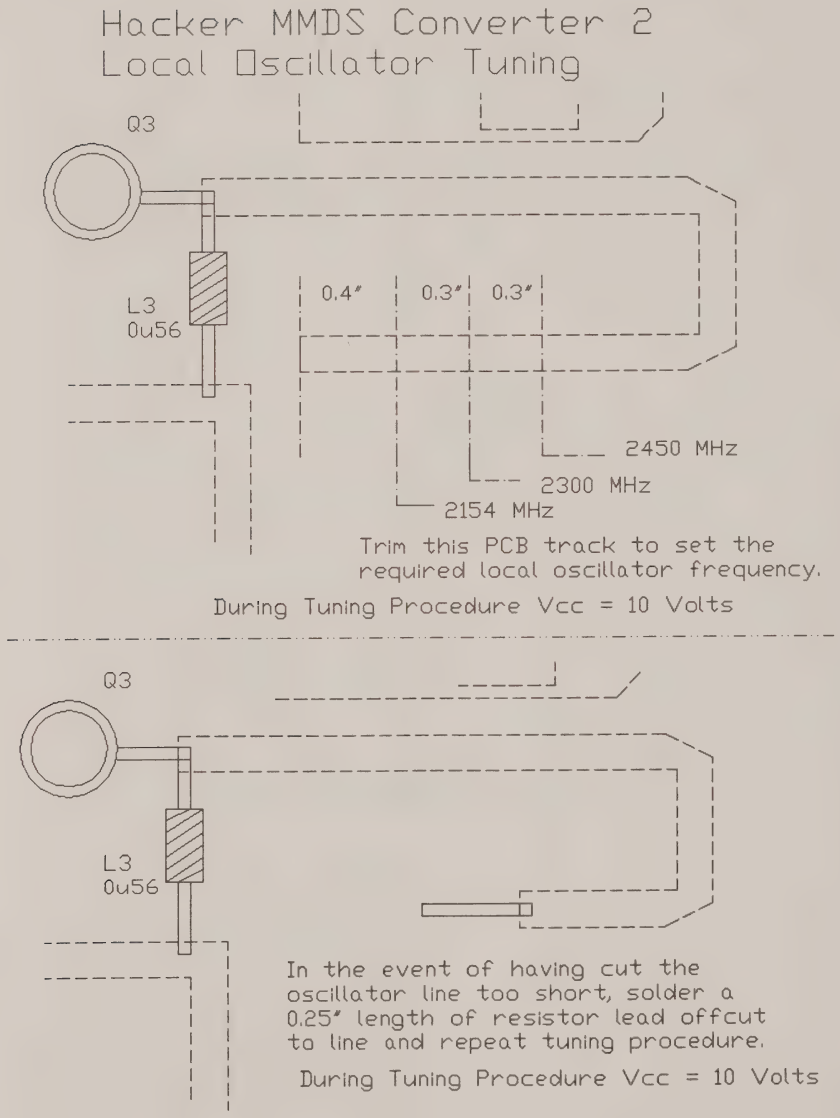

Hacker MMDS Converter 2
Input
Output
10u
470R
470R 10u 1n0
1n0
51R
100K
22K
1n0
0u56
0u1
1n0
NE64535
or NE02135
NE02137
MBD101
or
ND4981-7E
0u56 = 560nH
0u1 = 100 nH
1n0
2k0
1n0
2K7
1k0
NE02137
* = Component is part
of PCB track.




A
B
R8 2K7
C8 1nO
C7 1nO
R6 2K
Q3
R7 1KO
L3 0µ56
C6 10µ
C5 1nO
L2 0µ56
470R
R4
Q2
1nO
C4 1nO
C9
R5 22K
L1 0µ1
D2
D1
C2
C1
R1
Q1
100K
R2
51R
R3 470R
C3 1nO



Ensure that TV socket is isolated.


Hacker MMDS Converter 2
Local Oscillator Tuning
Q3
L3
0u56
0.4"
0.3"
0.3"
2450 MHz
2300 MHz
2154 MHz
Trim this PCB track to set the
required local oscillator frequency.
During Tuning Procedure Vcc = 10 Volts
Q3
L3
0u56
In the event of having cut the
oscillator line too short, solder a
0.25" length of resistor lead offcut
to line and repeat tuning procedure.
During Tuning Procedure Vcc = 10 Volts

Oscillator Alignment

The easiest way to set up the downconverter is by use of offair signals. A the present, this is not possible. There is an alternative method.

The irradiated tuned line method has been widely used by radio amateurs to set up microwave oscillators. A piece of copper wire, (the inner wire of a coaxial cable), is stretched over a groundplane such as a piece of unetched PCB material. The distance between the wire and the groundplane is approximately 2 mm.

One end of the wire is soldered to the ground plane. The other end is soldered to an OA91 or similar germanium diode. The other end of this diode is soldered to a 200 uA microammeter.

The line is irradiated by the signal from the local oscillator. By sliding a screwdriver along the line, the meter will indicate a series of lows and highs. These readings correspond to the troughs and peaks of the signal. By measuring the distance between the peaks, the frequency of the oscillator can be calculated. The formula is expressed below.

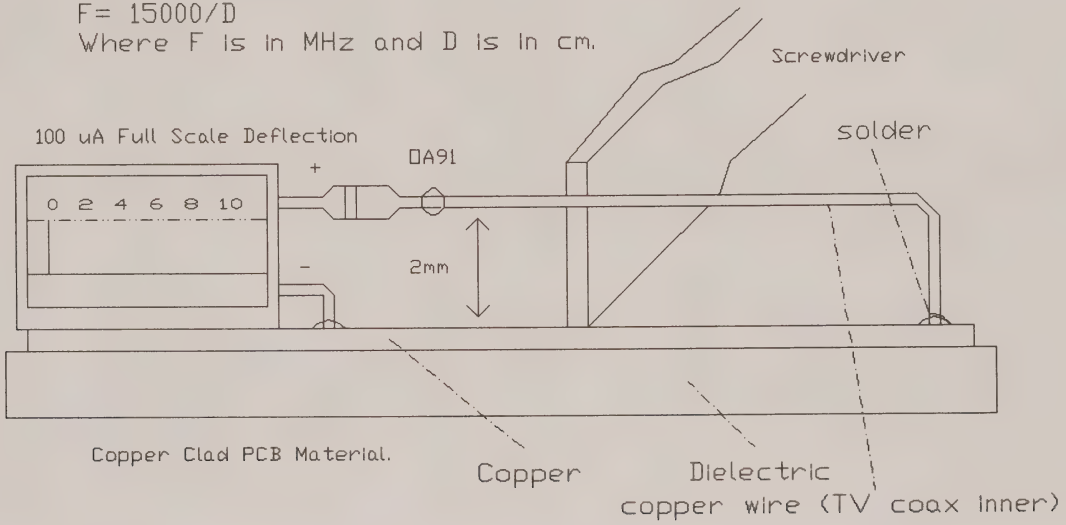
$$Fo = 15000/D$$

Where Fo is the oscillator frequency in MegaHertz and D is the distance between troughs in Centimetres.

Checking Microwave Oscillator Frequencies

The frequency of a microwave oscillator can be measured by irradiating a tuned line and measuring the distance between troughs or between peaks on the meter readings. The screwdriver tunes the line by shorting it to ground.

F= 15000/D
Where F is in MHz and D is in cm.



One of the best sources of antenna designs for MMDS is the RSGB VHF And UHF Manual. This book contains a number of antenna designs that are easily adapted for MMDS use.

A number of antennas can be built for use with the hacker converter. The ones covered in this chapter are as follows; the parabolic dish, the corner reflector, the ring Yagi, the helical and the "ray gun".

The Parabolic Reflector

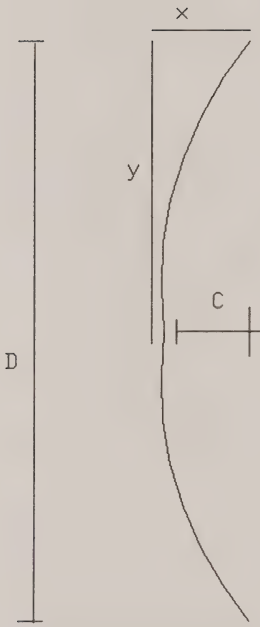
The parabolic antenna as used for satellite television reception can be used for MMDS. This is a rather expensive use of a dish. The reflective surface of a dish for use at MMDS can be mesh. The main factor governing the mesh gap is that it must be less than one eighth of the freespace wavelength of the lowest frequency of operation. Quarter inch wire mesh could be used. It is better to use the galvanised type rather than uncoated steel. The necessary formulae are given in the diagram. The gain of the parabolic is depends on the diameter and the operational frequency. With the launch of Astra, smaller dishes will be widely available at a low cost. For a gain of 22 dBi at 2.5 GHz, a 64 centimetre diameter dish is required.

The Corner Reflector

The corner reflector essentially consists of two parts; the dipole and the reflector. The reflector is simply an angled piece of metal sheet or metal mesh. The gain of the antenna depends on the angle of the reflector bend. A large number of the American designs that have been published have disregarded one essential fact-the feed impedance of the antenna. As the angle of the bend decreases, the gain increases but the feed impedance decreases. The easiest angle to match to is an angle in the region from 60 to 90 degrees. The closer the angle is to 60 degrees the better. Matching is carried out by varying the distance of the feed dipole from the centre of the angle. This distance, measured in fractions of a wavelength, is marked S in the diagram. For a 50R match, the range of S for the 60 degree angle is 0.41 to 0.49. For the 90 degree angle, the range is 0.3 to 0.35.

This is the easiest antenna type to fabricate and as such it will be one of the most widely used. It does not have significant

Parabolic Reflector



Gain dBi= 10 log(n*(((pi*D)/l)^2)

n= efficiency (typically 0.5)

l= wavelength in metres

D= diameter in metres

f= focal distance

c= depth of curve

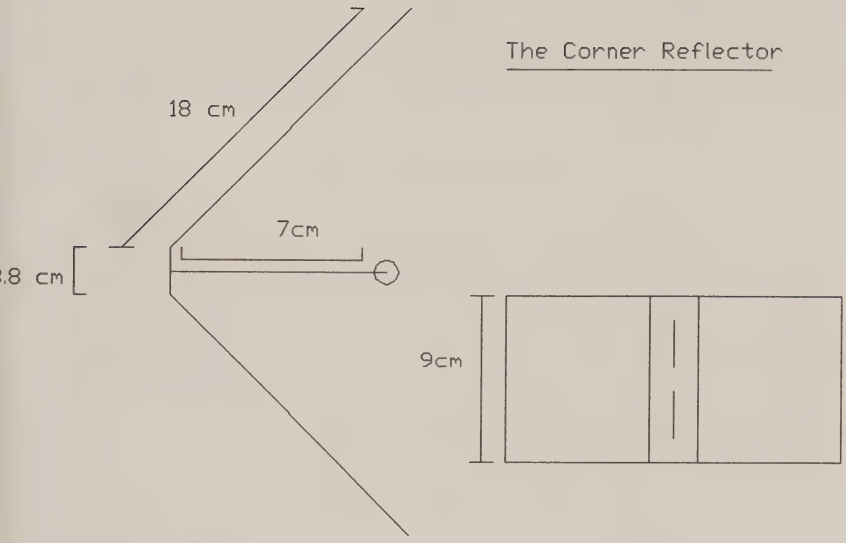
Equation: Y^2 = 4fx

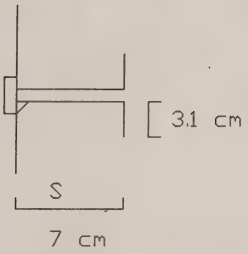
Focal Length, f= D^2/16c

Materials.

The surface accuracy of the reflector must be better than 1/8 th of a wavelength at the lowest operating frequency. Chicken wire mesh can be used for the application.

There are a number of methods used to construct this antenna type. The simplest is to cut a template from plywood and then cut a number of ribs, normally eight, from a sheet of marine plywood. The ribs would then be assembled into a spider and the mesh attached with staples. A cheap satellite dish could also be used.





Materials.
The relfector is aluminium sheet.
The dipole is 8 AWG copper wire.
One section of the dipole is soldered to the centre pin of an N type or BNC type connector. The other section is soldered to the connector fixing nut.

integral strength. It may not stand up to any severe winds. Therefore it would be better fabricated from wire mesh.

The Ring Yagi Antenna

The ring Yagi design presented here is one that has been used by hackers in the United States for the reception of MMDS. There should be no problem in obtaining any of the components for this antenna. The driven element is made from a strip of copper and the reflector and directors being fabricated from aluminium strip of 3/10 inch thickness.

The Helical Antenna

The helical antenna is essentially a coil of wire wound on the outside of a plastic pipe. The main equations governing this type of antenna are given in the diagram. This antenna offers 12dBi gain for a seven turn helix. The impedance of such an antenna would be in the region of 140R and requires a quarter wavelength transformer to match it to the input impedance of the converter. Ideally low loss insulators should be used to hold the helix rigid but the plastic tube is a readily available, though lossy compromise.

The Ray Gun Antenna

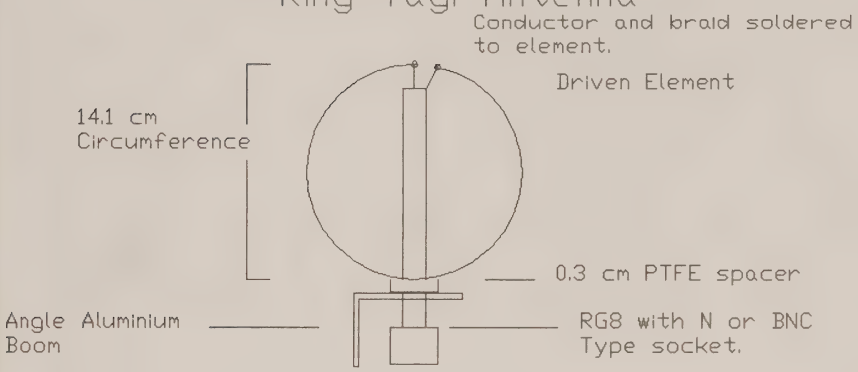
The ray gun antenna can be thought of as a ring Yagi with solid directors. The primary difference between this and the ring Yagi described earlier is the feed method. The "ray gun" is fed using a wave guide arrangement. The waveguide can be fashioned out of a 1lb tin can of the type used for catering. This wave guide without the "ray gun" assembly can give a gain in the region of 10dBi.

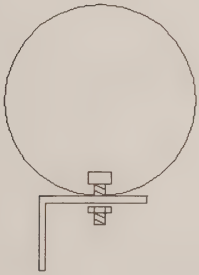
The Funnel Antenna

A further antenna type is the cone or funnel. The basis of this type of antenna is a cone of wire mesh on the tin can waveguide. The cone can be solid if required. A gain of 16 to 17dBi is possible with this antenna. When assembled, this antenna looks like a smoke stack on a chimney. This type of antenna has been used successfully by some American hackers. The people who worked for the MMDS companies couldn't tell them from real smoke stacks.

The first MMDS system in Ireland was hacked during the test

Ring Yagi Antenna


Conductor and braid soldered to element.
Driven Element
14.1 cm Circumference
0.3 cm PTFE spacer
Angle Aluminium Boom
RG8 with N or BNC Type socket.



Reflector Element: 14.7 cm Circumference

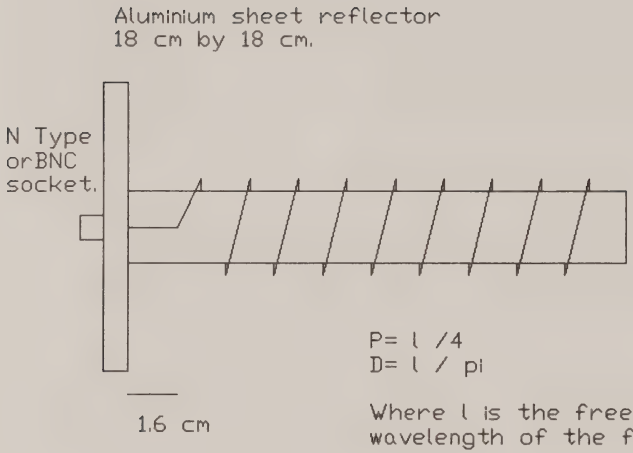
Director Element: 12.6 cm Circumference

All elements are formed from 3/16 " wide aluminium strip. Thickness is typically 20 SWG or 22 SWG.

S is a square aluminium sheet reflector of dimensions 6.8 cm by 6.8 cm.

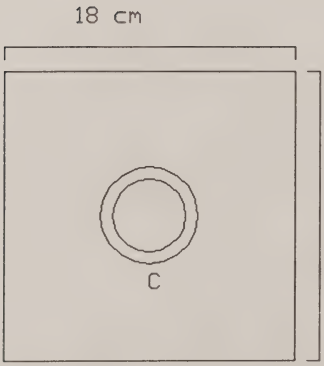
Distances:

a= 4.73 cm b= 1.45 cm c= 1.70 cm d= 1.20 cm
e= 2.70 cm f= 2.70 cm g= 5.40 cm



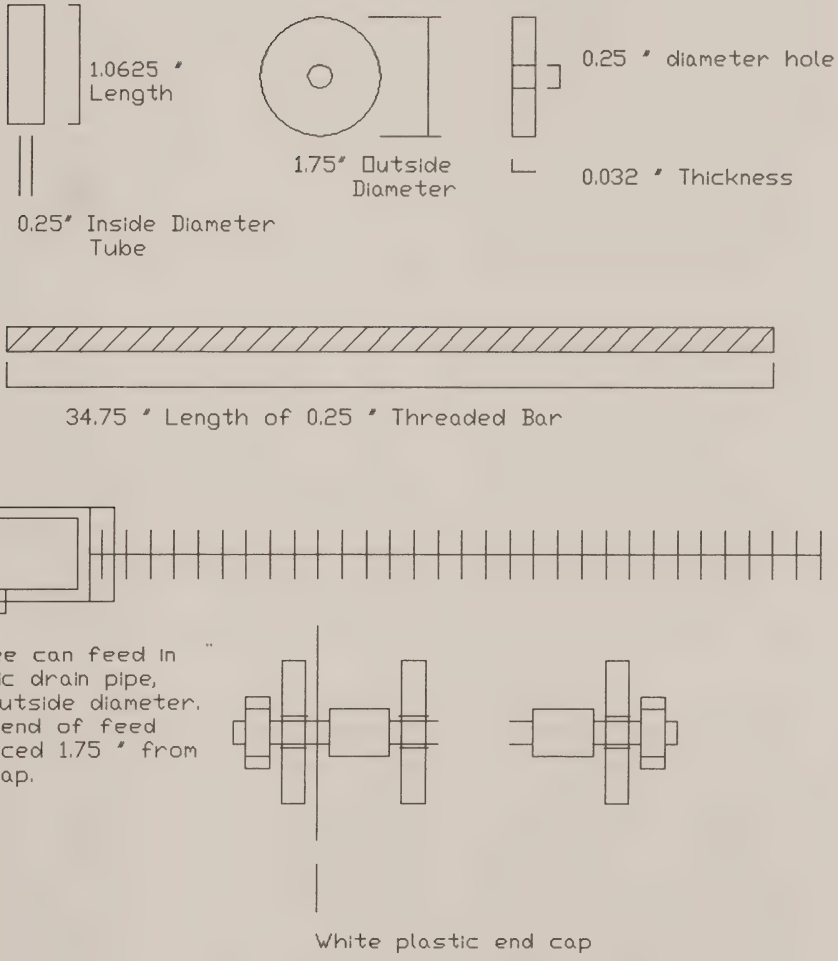
P= l /4
D= l / pi

Where l is the freespace wavelength of the frequency in use.

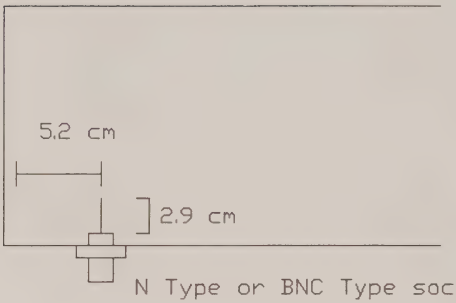


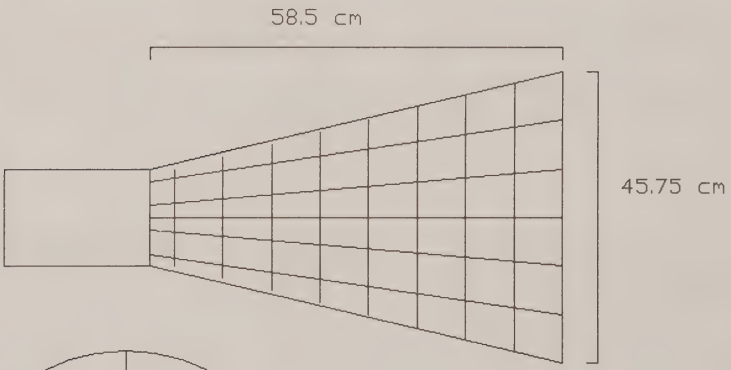
Materials.
The helix is made from 8 AWG copper wire. 1 3/4 " outside diameter plastic pipe is used to support the helix. The reflector is made from sheet aluminium, though mesh could be used.

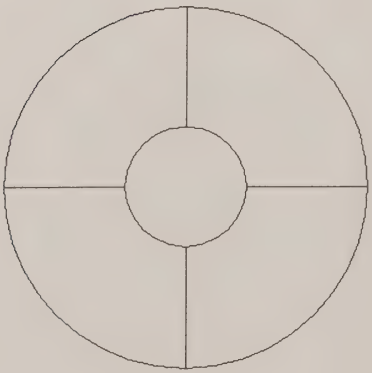
Ray Gun Antenna



Funnel Antenna







The funnel is constructed from quarter inch wire mesh over a rib structure. Four to eight ribs are necessary for ridgidity. The open end of the feed can be covered with a white plastic cover.

period using the hacker design given in Version 1 of this book. The signal was clear during the test period and it appears that it may be clear for at least the first six months of operation.

The MMDS service owners will have to teach their "installers" how to recognise the pirate or hacker antennas. Of course they will have to teach them how to install microwave reception equipment first. If they again begin to employ the well meaning amateurs as in the early days then MMDS in their area will almost certainly fail. If a similar policy of incompetants is employed at the transmitting end of the MMDS systems then it is only a matter of time before some of the people involved get their eyeballs fried by an incorrectly aligned microwave transmitter. Microwave transmission and reception is a highly specialised field. It requires both academic and practical skills. These skills will either have to be learned or bought in. Due to the time constraints involved, the buying in of these skills would be the most logical.

In the early days of QDBS satellite television in Ireland, every satellite television dealer was struggling to keep their business going. Then Cablelink and some of the other cable companies put the most boring channels available on their nets. The majority of people were treated to repeats that were already being repeated on terrestrial television. People then got the wrong idea about satellite television. The situation was not helped by the channels being available on the nets without charge. There were actual rumours of people involved in the cablenets giving out disinformation in order to stunt the sales of TVROs. A more likely explanation was that the people just didn't know what they were talking about.

Payback is just another word for revenge. Many of the present technical people of the satellite television industry cut their teeth on the C-Band. Most will look upon selling pirate MMDS equipment as getting even with the cable companies. It is very difficult to be unbiased when you have seen your friends lose their jobs and companies because of the actions of those who see the satellite television industry as a threat. The attitude prevailing at present among some of the more extreme Irish hackers can be summed up in one expression: You f%^$@ with us and we'll f%^$@ you up. From what I have seen of the satellite television industry, some of the cable companies have set themselves up as targets.

The reason for the use of the 61.25 MHz IF in the American hacker downconverters. The majority of the American MMDS systems employ scrambling systems. Many of these systems are synch manipulative and therefore it is not necessary to completely demodulate the signal. The descrambling can be achieved by a gain controlled amplifier.

In Ireland, the official scrambling system specification for an MMDS system does not permit synch manipulative systems. Of course there are exceptions but the majority of the systems in use are VMS.

There are some heated debates taking place regarding MMDS. Many of the existing rebeam operations will be closed down when the local MMDS franchise goes into operation. This has irritated many people. The rebeam operations are cheaper. In some areas they are genuine community services. The people living in the area funded the rebeam operation. In others, some people masquerading as representing the community while the only thing that they are representing is their bank balance.

The main question relates to the success of MMDS in Ireland. Will it be a failure? At this stage it is too early to tell. The main demand is for the UK channels. The majority of the rebeam operations only rebeam the UK channels. The MMDS franchise has to overcome the cost threshold. Their prospective customers have already spent about £100 for the UHF antenna and amplifier installation. Commonly the yearly subscription is £52 or about £1.00 a week. In some rebeam operations, old age pensioners are not charged for the service.

The perception of the MMDS franchise operators is one of a cold dispassionate bizoid structure whose only aim is profit. While this is not the case with all franchise operators, the image is promoted by rebeam operators.

MMDS will be successful in some areas. The terrain of Ireland is not conducive to MMDS. Some areas are too hilly for proper coverage. Other areas are too heavily wooded. In my opinion, MMDS is an antique. Satellite can provide a better coverage and some good scrambling systems exist to provide reasonable security. With the newer digital compression systems, regionally sectored packages would be feasible.

9: Descrambler Hook Ups

At the uplink to the satellite, the television signal is pre-emphasised and has a dispersal waveform added. The reasons for these modifications are simple. The pre-emphasis improves the signal to noise ratio of the received signal. The function of the dispersal waveform is twofold. It prevents the satellite transponder from being damaged and it prevents interference with terrestrial microwave links. The latter aspect dates back to the dual use of C-Band in the United States.

The output of the demodulator in the satellite television receiver is termed baseband. The bandwidth of baseband is generally 50 Hz to 8 MHz. The MAC baseband bandwidth is generally 50 Hz to 10 MHz. It is unfiltered and it contains the video signal and the audio subcarriers. Since the required video bandwidth for PAL-I is 5.5 MHz, (PAL-G is 5.0 MHz), the video and the audio carriers must be separated for processing.

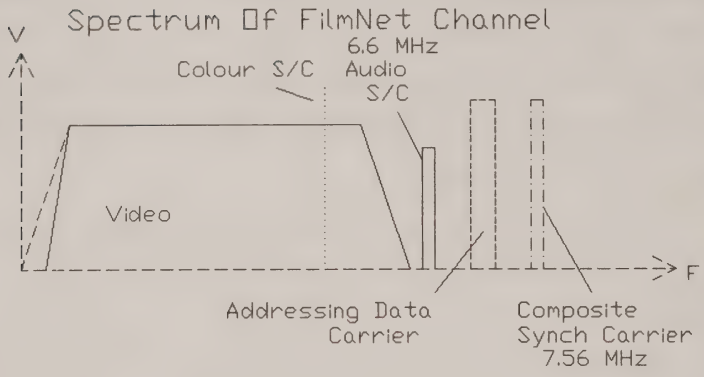
Filtering

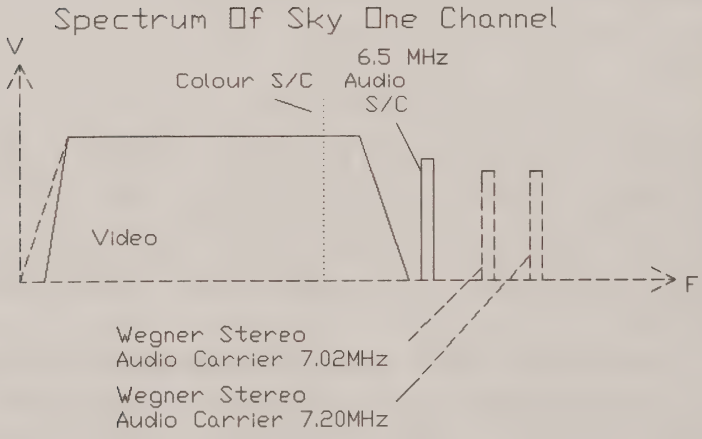
The video filter in the satellite television receiver allows the signals below 5.5 MHz to pass but stops the higher audio subcarrier frequencies. The audio subcarrier frequencies on satellite transmissions generally occupy the 6.0 to 8.0 MHz bandwidth segment. Many of the receivers used on ASTRA are modified from those designs used on the American market. These receivers can be recognised by the fact that their audio subcarrier tuning range is 5.0 MHz to 8.0 MHz.

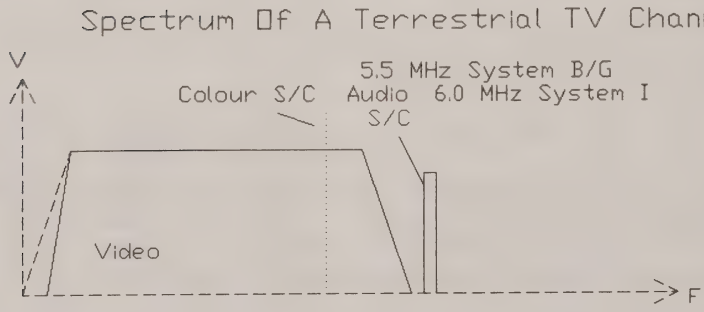
The audio subcarriers are passed by means of a high pass filter to the audio demodulators in the satellite television receiver. The high pass filter will drastically attenuate the video frequency components in the baseband signals. It is important that the audio subcarriers present in the baseband signal are attenuated when using a descrambler with its own integral remodulator. With some types of remodulator, the unattenuated subcarriers cause interference on the descrambled video.

Pre-Emphasis And De-Emphasis

The noise spectrum of an FM signal is triangular. As the frequency increases the amount of noise increases. This means that the colour components of the satellite television signal will be noisier than the lower frequency luminance components.


Spectrum Of FilmNet Channel
V
6.6 MHz
Colour S/C
Audio
S/C
Video
F
Addressing Data
Carrier
Composite
Synch Carrier
7.56 MHz


Spectrum Of Sky One Channel
V
6.5 MHz
Colour S/C
Audio
S/C
Video
F
Wegner Stereo
Audio Carrier 7.02MHz
Wegner Stereo
Audio Carrier 7.20MHz


Spectrum Of A Terrestrial TV Channel.
V
5.5 MHz System B/G
Colour S/C
Audio
6.0 MHz System I
S/C
Video
F

Pre-Emphasis is the process whereby the high frequency components of the signal are boosted with respect to the lower frequency components of the signal. If the satellite television picture is displayed without de-emphasis, it will appear sharper in contrast and definition. In the not too distant past, some of the amateur descrambler manufacturers touted this improved definition as a product of their descrambler. According to some reports, this practice persists.

De-Emphasis is the reverse of the pre-emphasis. The high frequency components of the signal are attenuated by an inductor - capacitor - resistor network. The values of the components in this network ensures that the high frequency components are affected and the low frequency components are passed with minimal attenuation.

Dispersal Waveforms And Clamping

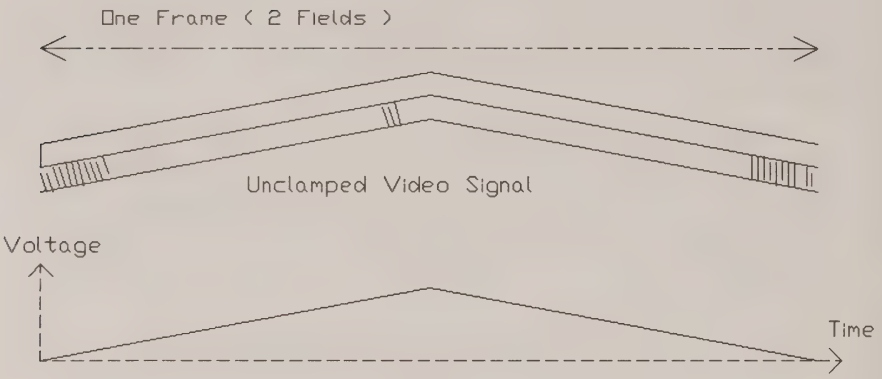
The widespread use of C-Band in the United States as a satellite allocation and terrestrial allocation meant that there was a possibility that interference could occur. Satellite transponders were also extremely delicate and prone to failure. If a black or white level was transmitted on a vacant transponder, the concentration of RF energy in one section of the spectrum could cause the transponder to fail. The solution to the problem was dispersal.

On European satellite television, a 25 Hz triangular waveform is generally used. A satellite television picture when displayed without clamping will flicker on the screen.

The clamping circuit in the satellite receiver generally clamps the video by using a Zener diode and Schottky diode combination. Sometimes the manufacturer will economise and use an ordinary silicon diode such as a 1N4148 or a 1N914.

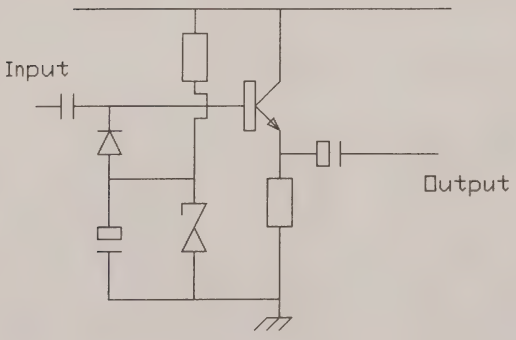
The video signal supplied to a descrambler must, in the majority of cases, be unclamped. The descramblers generally have their own clamping circuit but this is not the reason for the unclamped video. In the case of active video inversion, the black levels of the inverse video and the normal video are different. The descrambler will have a preset to null the difference. In clamped video, the black level of the normal video would be correct but the black level of the inverse video would be dependent on the peak

Dispersal And Clamping



The dispersal waveform is a field locked triangular waveform. This ensures that the energy concentration on a black level only transponder is spread or dispersed over a range of frequencies rather than concentrated at a few frequencies. A secondary reason for the addition of the dispersal waveform is that the C-Band frequencies are used by satellite and terrestrial services. A satellite transmission without dispersal would create a possible interfering carrier on the terrestrial service. The dispersal concept has it origin in the USA.

A Tyical Clamp Circuit



level of the video. Add the spectre of synch shifting to this and it really gets messy. The bright sections of the picture tend to smear and leave trails across the screen.

With sinewave based scrambling systems such as Sat-Tel's SAVE, the reason for unclamped video is different. The descrambler needs a perfect sinewave so that is can cancel the sinewave. Clamping the video prior to descrambling would flatten the sinewave and so there would not be proper cancellation. In the basic SAVE specification, the video is attenuated and inverted. The clamping action disturbs the synch pulses so that bright scenes tend to tear.

The ASTRA Receiver Specification

An ideal ASTRA satellite television receiver has the following characteristics;

Demodulation Bandwidth: 24 to 27 MHz

Overall Adjacent Channel Rejection: >25 dB

Frequency Tuning Range: 10.95 to 11.7 GHz

Demodulator Threshold: <9 dB CNR

Clear Sky Reception: >12 dB CNR

Rejection Of Energy Dispersal: >35 dB

The demodulation bandwidth is the cause of the majority of problems with the older receivers. Some of the older receivers use a bandwidth of 30 MHz. This causes an image of an adjacent channel in the background of a received channel.

The frequency tuning range is the full Ku-Band. Some of the 16 channel models will not be able to store the full 48 channels that will be available via ASTRA in 1993. Most receivers are capable of this bandwidth as receiver manufacturers have in most cases modified an existing full band receiver to the ASTRA specifications.

The demodulator threshold is less than 9 dB. This basically means that the receiver must be able to give good pictures down to a CNR of 9 dB. It has been the experience of most engineers that

the threshold specified on a data sheet is as reliable as a politician's promise.

Under clear skys operation, the receiver must give a CNR on a received signal in excess of 12 dB. This is regarded by many as a level approaching broadcast standard. The dish and LNB play an important part in this section.

The ASTRA Receiver Specification - Video / Audio Output

The video output of the ASTRA receiver should supply 1 Volt into 75R. The mono audio and or stereo audio should be available via sockets on the receiver. The choice of sockets is up to the manufacturer. The SCART connector is an option.

The ASTRA Receiver Specification - UHF Output

This specifies a remodulator with a tuning range of channel 32 to channel 40. The audio for the remodulator should be be selectable from the number of ASTRA audio carriers. The remodulator must also provide a facility for combining the off-air television signals with the remodulated output.

The ASTRA Receiver Specification - Decoder Interface

This is perhaps the greatest source of problems for the installer. The ASTRA specifications are sometimes ignored by manufacturers. One receiver in particular has used inverse logic where the official specification is for 0 or 12 volt logic. This means that some of the descramblers will not work on this receiver. Luckily, some descrambler manufacturers have incorporated a switch to allow for these types of receivers.

The main specification for the decoder interface requires that it has both PAL video and non de-emphasised non filtered baseband outputs along with the audio outputs. The objective is to ensure that the decoder interface is usable for the MAC decoders.

9: Descrambler Hook Ups

The interface must also have video and audio inputs for loop through. Loop through allows a transparent operation of the descrambler. If a scrambled signal is detected, the descrambler video and audio outputs are selected. If the signal is clear then the receiver outputs are used. The loop through is controlled by the video switch pin.

The official specification recommends the use of a sub-miniature D-Type socket. Some manufacturers have used a SCART socket in its place. In the standard terrestrial applications, the video signal used is clamped and filtered baseband. This is unsuitable for use in certain types of descrambler and the use of unclamped unfiltered baseband is recommended. The specification also points out that such a SCART should be labeled "DECODER ONLY".

The specifications also include the parameters for a MAC decoder output. The requirements are different to the ordinary type of descramblers. This is because the digital audio is included in the MAC signal. The filtering, de-emphasis and clamping would have an adverse effect on the video and digital information.

The ASTRA Receiver Specification - MAC Baseband

Baseband Response: 25 Hz to 10.5 MHz

Amplitude Response: +/- 2 dB 25 Hz to 8.4 MHz

+/- 3 dB up to 10.5 MHz.

Group Delay Response: +/- 25 nS

Signal Level Output: 1 Volt Pk to Pk (Adjustable)

Output Impedance: 75R unbalanced

De-Emphasis: Flat

Dispersal Rejection: Unclamped

9: Descrambler Hook Ups

The ASTRA Specifications For D-Type Interface

The D-Type socket is used on many ASTRA receivers for interfacing the descrambler with the receiver. The function of each pin is given in the text table.

Pin Connections Table:

Pin Number 1: Return Audio Input Left

Pin Number 2: Return Video Input PAL

Pin Number 3: Video Switch Signal

Pin Number 4: Baseband Output

Pin Number 5: Clamped PAL Video Output

Pin Number 6: Return Audio Input Right

Pin Number 7: Audio Signal Switch

Pin Number 8: Ground

Pin Number 9: RESERVED

Pin Number 10: RESERVED

Pin Number 11: Ground

Pin Number 12: Audio Output Left

Pin Number 13: Audio Output Right

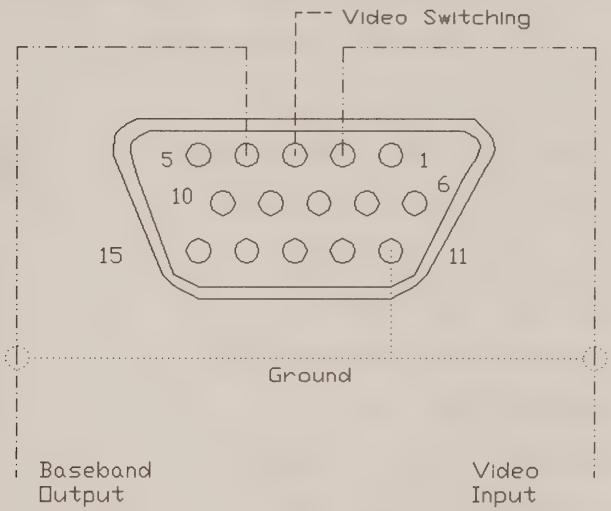
Pin Number 14: RESERVED

Pin Number 15: RESERVED

The video and audio switch pins select the respective descrambler outputs. If the video is scrambled and the descrambler has a valid output, then the Video Switch pin will at ground. If the video is normal PAL and the descrambler is not active, the video switch will be at 12 Volts. This causes the receiver to select the descrambler video.

D-Type Connections

As Viewed From Rear Of Receiver



Pin 3 is the video switching control. 12 V selects external source and 0V selects internal.

Pin 7 is the audio switching control. 12 V selects external source and 0 V selects internal. This pin is taken low by an internal resistor. Unless audio scrambling is in use this pin should be left unconnected.

ASTRA Specifications For SCART Descrambler Interface

The SCART socket is used on some receivers as a decoder interface. The use of loop through means that the operation of the descrambler is transparent and the customer will not ideally notice a transition from a clear station to a descrambled pay channel.

Pin Connections Table

Pin Number 1: Audio Output Right

Pin Number 2: Return Audio Input Right

Pin Number 3: Audio Output Left

Pin Number 4: Audio Ground

Pin Number 5: RESERVED

Pin Number 6: Return Audio Input Left

Pin Number 7: RESERVED

Pin Number 8: Audio/Video Switch

Pin Number 9 - 16: Reserved For Other Applications

Pin Number 17: Video Output Ground

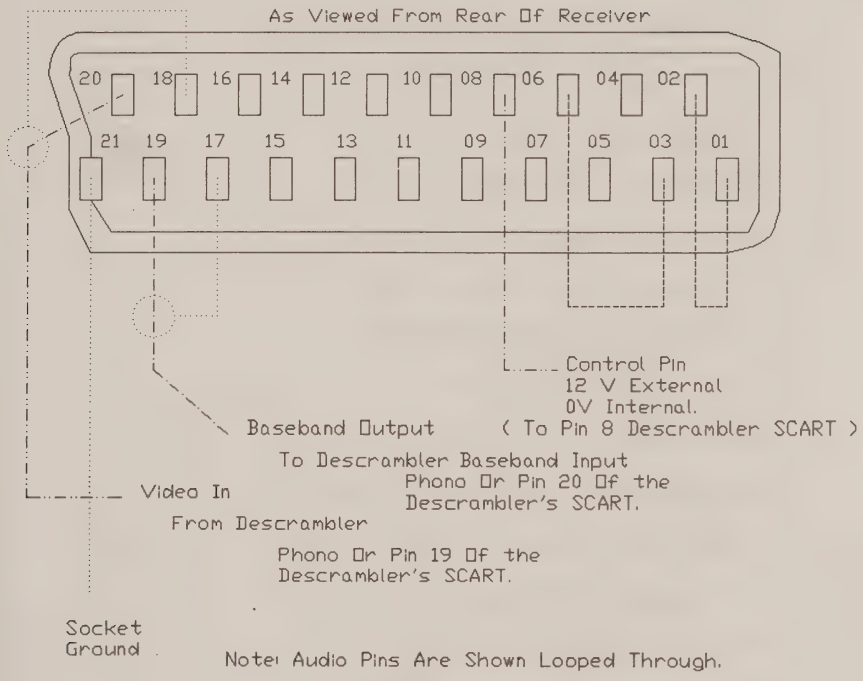
Pin Number 18: Video Input Ground

Pin Number 19: Baseband Output

Pin Number 20: Return Video Input PAL

Pin Number 21 Common Ground

Decoder SCART Connections


As Viewed From Rear Of Receiver
20 18 16 14 12 10 08 06 04 02
21 19 17 15 13 11 09 07 05 03 01
Control Pin
12 V External
0V Internal.
Baseband Output
(To Pin 8 Descrambler SCART)
To Descrambler Baseband Input
Phono Or Pin 20 Of the
Descrambler's SCART.
Video In
From Descrambler
Phono Or Pin 19 Of the
Descrambler's SCART.
Socket
Ground
Note: Audio Pins Are Shown Looped Through.

Pin 4 is Audio Ground.
Pin 17 is Baseband Output Ground
Pin 18 is Video Input Ground

9: Descrambler Hook Ups

Standard SCART Interface

The SCART socket is used on some receivers to connect directly to a video recorder or television.

Pin Connections Table

Pin Number 1: Audio Output Right

Pin Number 2: Return Audio Input Right

Pin Number 3: Audio Output Left

Pin Number 4: Audio Ground

Pin Number 5: Blue Return

Pin Number 6: Return Audio Input Left

Pin Number 7: Blue Input Or Output

Pin Number 8: Audio/Video Switch

Pin Number 9: Green Return

Pin Number 10: Not Connected

Pin Number 11: Green Input Or Output

Pin Number 12: Not Connected

Pin Number 13: Red Return

Pin Number 14: Not Connected

Pin Number 15: Red Input Or Output

Pin Number 16: Blanking

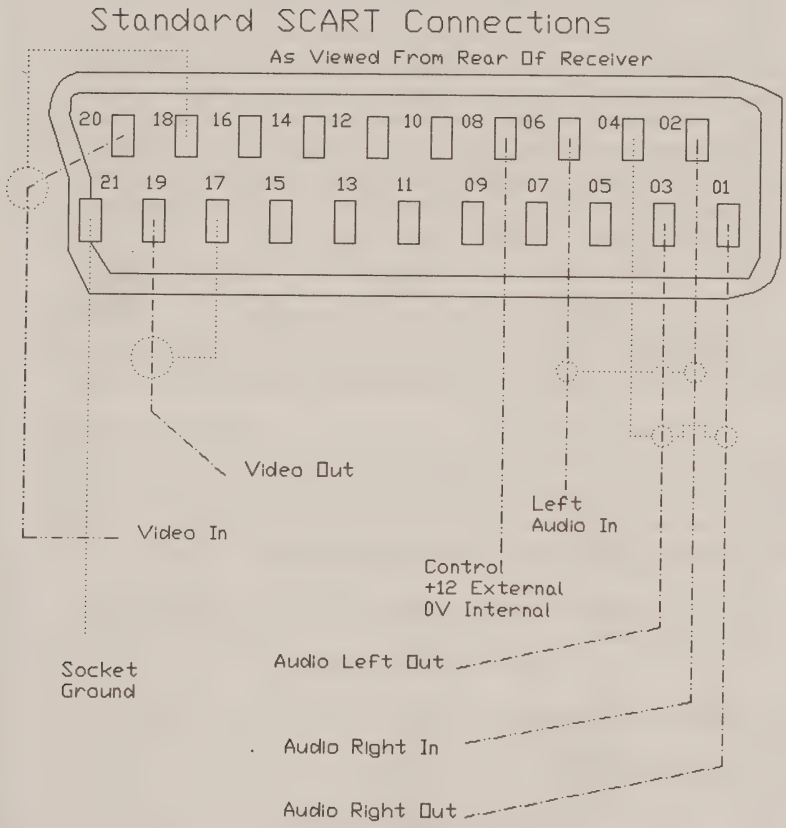
Pin Number 17: Video Ground

Pin Number 18: Blanking Ground

Pin Number 19: Video Output

Pin Number 20: Video Input

Pin Number 21 Common Ground



Pin 4 is Audio Ground.
Pin 17 is Video Output Ground
Pin 18 is Video Input Ground

9: Descrambler Hook Ups

What Exactly Is Loop Through?

There is still a lot of confusion as to the exact nature of Loopthrough. To many it merely means that a descrambler can be connected to the receiver. The descrambler will then almost magically switch itself into operation when the correct scrambled channel is selected.

The purpose of loopthrough is to enable the receiver to accept a video source other than the output of its own demodulator. The alternative video source is then routed to the satellite television receiver's remodulator. It is also possible to route the audio in this fashion.

The source selection is determined by PIN 8 on the SCART. The voltage on this pin will be high, 12V, when the descrambler is in operation. When it is low, the receiver selects the internal video.

On the Sakura receivers, the reverse of the normal situation is applied. For the descrambler video to be selected, PIN 8 must be pulled low. Many of the more recent descramblers have provisions for these receivers. In cases where there is no provision for this inverse switching, a separate lead has to be made.

The main requirements for loopthrough are stated below.

Descrambler Inputs:

Baseband Or Unclamped Video

Audio (Optional)

Descrambler Outputs:

Descrambled Video 1V pk to pk

Descrambled Audio (Optional)

Switching Signal [PIN 8] Normally Active High

9: Descrambler Hook Ups

Loopthrough Type 1:

Video Output:- Straight Through When Inoperative

The first loopthrough type allows the signal seen at the descrambler input to pass unmodified to the descrambler output when the descrambler is inactive. This means that if the input to the descrambler is baseband then baseband will appear at the video output of the descrambler when the descrambler is inoperative. This is the ideal type of loopthrough for chaining or parallel descrambler connection.

A descrambler with this type of loopthrough is unsuitable for use with a receiver that has not been modified for loopthrough. Most of the old SMATV receiver / remodulator combinations cannot use a descrambler with this loopthrough type. The displayed video would be unclamped video or raw baseband depending on the input.

Loopthrough Type 2:

Video Output:- Processed Video When Inoperative

This loopthrough type process the descrambler input so that a de-emphasised, filtered and clamped video signal appears at the video output of the descrambler.

This type of loopthrough is acceptable for use on a SMATV receiver / remodulator combination as described above. It is also suitable for use on unmodified receivers where a video recorder is used as the remodulator. This is how it used to be done in the days before ASTRA and sometimes this technique is still used where the receiver is of pre-ASTRA vintage.

It is obviously not suitable for parallel operation. When a descrambler with this type of loopthrough is run in parallel with a passive double SCART lead, the receiver is forced into accepting both the descrambled video and the video from the inoperative descrambler. The effect on the screen is one hell of a mess.

Loopthrough Type 3:

Video Output:- No Output When Inoperative

This type of loopthrough has no video output when the descrambler is inoperative. This would mean that it is suitable for chaining. It cannot be used on the SMATV receiver / remodulator combination as there will be no picture when the channel is not scrambled. While this may be Ok for a channel like Sky movies, it is not acceptable for FilmNet. FilmNet goes clear for about half an hour at various times throughout the day.

Determining The Loopthrough Type

The main piece of test gear required for this procedure is an oscilloscope. The other elements required are the receiver and the descrambler.

The cover of the one of the SCART connectors on the loopthrough lead should be removed. The oscilloscope probe should be connected to the video input line. This is the line that carries the descrambler video to the receiver.

The receiver should then be tuned to the scrambled channel. If the descrambler is operating properly, PIN 8 should be high. This can be checked with a multimeter.

The video input line should be carrying clamped descrambled video. If it is not check that the descrambler is operating properly.

Select a clear channel on the receiver. The control pin, PIN 8, should be low and the video line signal on the scope will conform to one of the loopthrough types listed.

Chaining Descramblers

The use of different scrambling systems means that there will be a number of descramblers to be connected. The most common descramblers are Sky and FilmNet. This of course is a source of irritation to Sky as the FilmNet descramblers are pirate types.

9: Descrambler Hook Ups

Chaining descramblers essentially allows the receiver to use a number of descramblers. It is a parallel operation as opposed to a serial operation. As with any method of hooking up electronic equipment, there is more than one way.

Before attempting to chain descramblers, the loopthrough type must be established. This is essential if the right type of connectors are to be used.

There are three types of connector that can be used for chaining descramblers; the SCART to SCART lead, the double SCART lead and the active switching box.

The SCART to SCART Lead

Descrambler Loopthrough: Type 1

This type of connection is really only suitable for the connection of one descrambler.

The Double SCART Lead

Descrambler Loopthrough: Type 3

This type of lead has one connection for the receiver and two other SCARTs. The other SCARTs allow for the connection of two descramblers. Since the SCARTs are wired in parallel, there should be no video output from each descrambler when it is inoperative.

This connector should not be used with descramblers with Type 1 or Type 2 loopthrough.

Active Switching Box

Descrambler Loopthrough: All Types

The active switching box allows a receiver to select the output from a number of descramblers. It also provides isolation from the unselected descramblers by operating an EXclusive OR function on the descrambler outputs. This means that only one source can be selected at a time. Thus if two descramblers go operational at the same time, none of the descrambler outputs will be selected. The

actual circuitry of such a unit is relatively straightforward. The better units use relay switches though standard 4066 CMOS switches can be used. The control signal from each input, (descrambler), SCART socket is fed to an EXOR gate which determines which input will be selected for loopthrough to the receiver.

Modulators And VCRs

The majority of video recorders have direct video connections. The user can connect a direct video source such as a camera and take the direct video output of the VCR to a monitor for better quality pictures.

Descramblers or decoders can make use of this facility. In many cases, the use of the VCR as a modulator is necessary. Direct video input on television receivers is more of a recent trend. It is not unusual to find a customer with the latest model VCR and an old television set.

To use a VCR as a modulator is not difficult. The procedure is generally covered in the VCR manual. There is a deal of uniformity between the procedure as used on different VCRs. Generally the VCR has to be set to channel 0 or AUX. Sometimes there is a Video Camera input that can be used.

If a number of different brands of receivers are installed in the course of business it is better to build up some form of database on the types of connector used on each receiver. Since many European installers will also have a video and television section in their business, it would be useful to keep a list of the video and audio connector types on the VCRS direct input televisions. A sample chart is shown below.

Sample Connector Chart

Satellite Receiver .....

Video Out Connector .....

Audio Out Connector .....

Descrambler .....

Video In Connector .....

Audio In Connector .....

Video Out Connector .....

Audio Out Connector .....

Video Cassette Recorder .....

Video In Connector .....

Audio In Connector .....

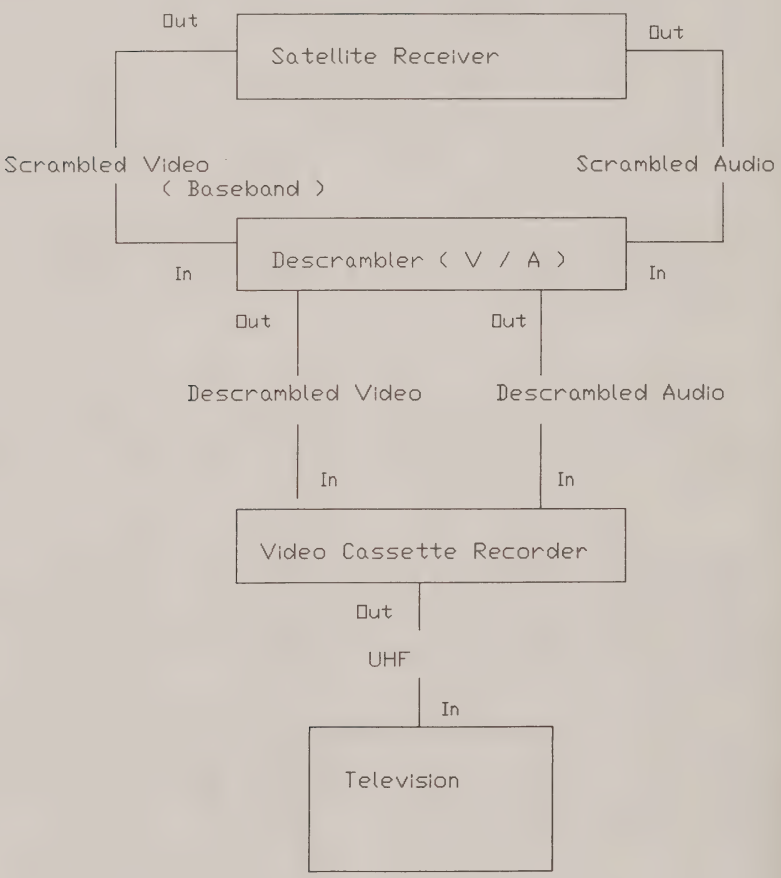
The use of the connector database would save time and effort on descrambler installations. If the installer has this information to hand at the office or the shop, then he can prepare the necessary connector kit before setting out on the installation. The alternative is to carry a video and audio connector interface kit on each installation.

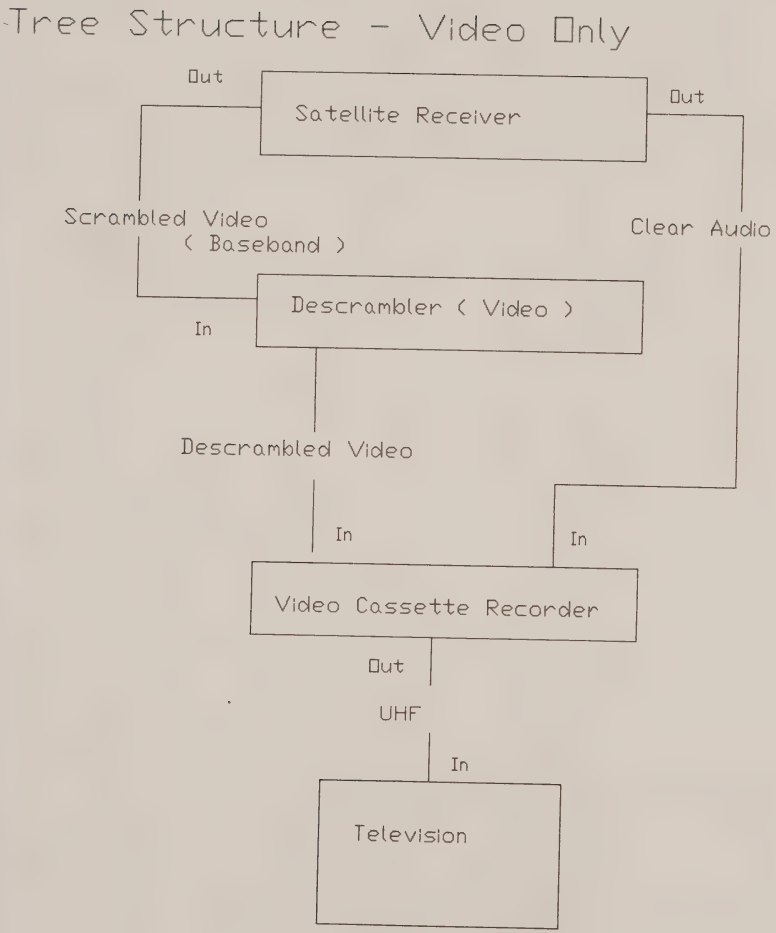
A tree structure procedure can then be used for the descrambler installation. As the installer completes each connection, the relevant lead is ticked off on the chart. This gives the installer a record of the installation details which could be useful if there is ever a service callback.

It should also be noted that the satellite television receiver and the VCR modulator channels are included on the charts. Some sources recommend that a two channel spacing. This spacing is a bit close for anything other than crystal controlled modulators. In practice the separation should be greater than two channels.

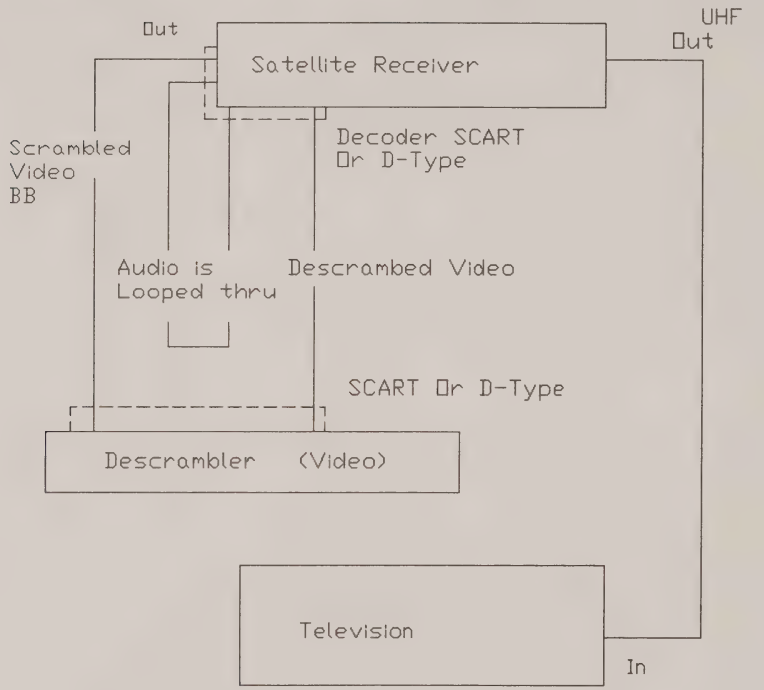
The use of computers in other areas of the house can actually cause interference problems. Some of the popular makes of home computer contain noisy modulators that work on UHF. This should be checked at the time of installation. If it is not, it could lead to a service call out.

Tree Structure - Video And Audio




Tree Structure - Video Only
Out
Satellite Receiver
Out
Scrambled Video
(Baseband)
Clear Audio
Descrambler (Video)
In
Descrambled Video
In
In
Video Cassette Recorder
Out
UHF
In
Television

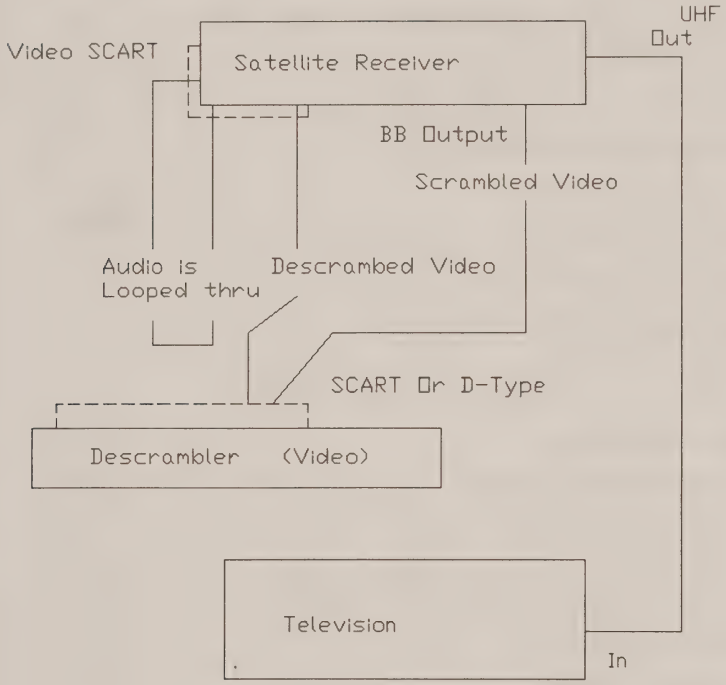
Tree Structure - D-Type Or SCART



The leads shown are parts of the SCART or D-Type lead. The control pin lead is not shown in the diagram above.

The audio lead must be looped through on the SCART lead to ensure there is a Return Audio signal. For video and audio descramblers the audio output of the receiver goes to the descrambler. The return audio signal should be that of the descrambler.

Tree Structure - Video SCART/ BB



The receiver's baseband ouput is used to feed the descrambler. The control pin lead on the SCART lead is not shown. This tree uses the receiver's VIDEO SCART.

The audio lead must be looped through on the SCART lead to ensure there is a Return Audio signal. For video and audio descramblers the audio output of the receiver goes to the descrambler. The return audio signal should be that of the descrambler.

Distributors Of MC2 Books

Ireland & EC (excl UK)

MC2 (Publications Division),

22 Viewmount, Waterford.

Voice & Fax: 051-73640

Int +353-51-73640

UK

J. Vincent Technical Books,

24 River Gardens, Purley

Reading, RG8 8BX

Voice & Fax: 0734-414-468

Mobile: 0836 582 785

Sweden & Scandinavia

Emerald Electronics,

Box 1342, S-181 25 Lidingo

Primary UK Retailer

Swift Publications,

17 Pittsfield, Cricklade

Swindon, Wilts, SN6-6AN

Voice & Fax: 0793-750-620

Smart Card Security

At this stage in time it is very difficult to be positive about the security of smart cards. Those in favour of their security are generally some way involved in selling the cards. It is a cynical viewpoint that is tempered by experience. Most of the smart card based scrambling systems in Europe have been hacked.

This section deals with smart cards. Or to be more precise, it deals with the technology and the hacks. Some of the material here is drawn from the previous versions but there new material. Some of it, the hacks perhaps, will cause embarrassment to the bureaucratic automata that traipse around claiming that their systems are totally secure.

Furthermore the section deals with most types of smart card including the memory cards as used payphone applications. While these cards have not seen use on satellite scrambling systems yet. There are some rumours that they will be used for special event programming. Such a move would be extremely unwise as the memory card is particularly vulnerable to hacking. The hacks covered range from the simple write voltage limitation to more elegant methods.

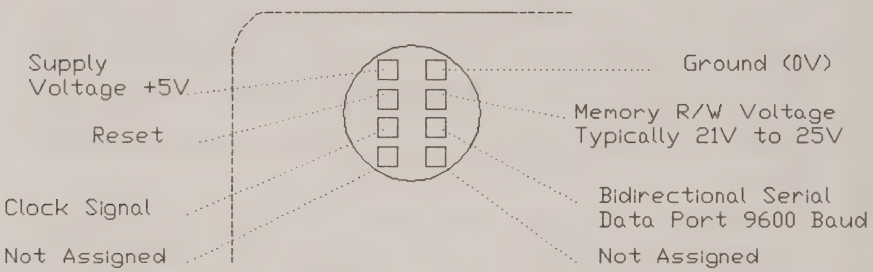
Some people may question my motivation for including information on telephone card. Perhaps they may consider it vengeance for high telephone bills. The reason is more mundane. There are rumours that the Pay Per View features that will be implemented by some channels will use a combination of these memory cards and real smart cards. The 8052 in the VideoCrypt decoder has routines that handle both smart cards and memory cards.

How Smart Is 'Smart'?

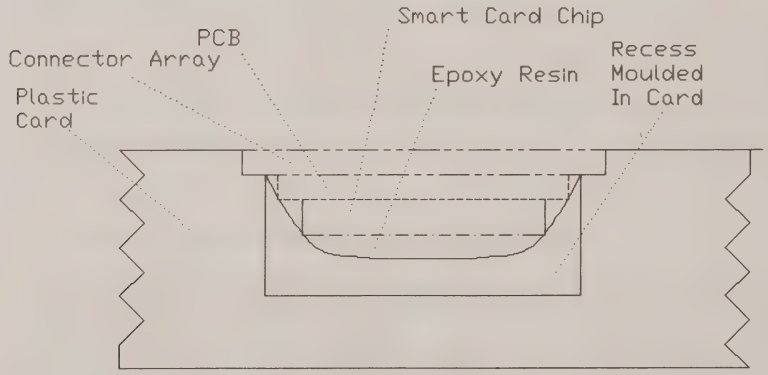
Smart cards are relatively cheap and ultimately disposable technology. The concept of disposable technology is a particularly modern one. Most countries in Europe have smart card payphone cards. There are of course countries like the UK that are using optical cards. In the USA there are some test programs using memory cards for payphone applications.

The problem with smart cards is that the term has become too generalised. It has to cover a few types of card. The phone card is generally a memory card but for the purposes of marketing, it becomes a "smart card".

The ISO Smart Card Standard Connector Functions.



Cross Section Of Smart Card



Perhaps the best definition of a smart card is a card that contains a microprocessor and memory. The memory cards used for pre-paid applications are, in this light at least, best viewed as dumb cards.

There are essentially two classes of smart cards; contactless and contact. The contact type smart card requires direct electrical connection to the card reader. In many respects this is the cheaper option. The interface circuitry is kept to a minimum.

The contactless smart card does not require a direct electrical connection to the card reader. Instead it uses a set of tuned circuits to pick up the signals from the card reader. Essentially three frequencies would be used. One frequency would be rectified to provide the card's DC supply voltage and the others would be used for data transmission.

Such complexity is not really suitable for Pay television applications. The cost is high and Pay television applications are often more concerned with getting the most efficient technology for a low price.

The contact type of smart card requires direct electrical connection between the pads on the cards and the decoder socket. There is an ISO specification governing the construction and connection protocols of smart cards - ISO-7816. Much of the information on the card protocols can be found in part three of this document.

The ISO Specifications - The Pads & Card

The connector specifications for the contact SMART card have been established as an ISO standard. The ISO standard specifies eight connections of which only six are actively used. Many of the SMART cards used for payphones and banking applications follow the pattern that appears in the diagram. The typical payphone card is an EPROM memory card rather than a smart card.

VideoCrypt's card does not look like it follows the pattern but it does have the same six connections on the connector array. Indeed the actual shapes of the pads on a card is an indicator as to the manufacturer of the card.

There are also some strict guidelines covering the position of the pads on the card and indeed the actual dimensions of the card. Most of the pirate cards are about twenty millimetres longer than the official cards. This is to facilitate the use of surface mount chips. Some of the

more recent decoders and IRDs have recessed card slots and this would cause problems as the chip would prevent the card from being fully inserted.

SMART Card Structure

The structure of the card is deceptively simple. It consists of a microprocessor and memory. This description fits the microcontrollers used to control receivers and video recorders and indeed it the same types of chips are used in these applications. The type of memory used can vary. It generally involves Read Only Memory, Erasable Programmable Read Only Memory, Electrically Erasable Programmable Read Only Memory and Random Access Memory.

The information stored in the ROM is fixed and cannot be altered without changing the design of the SMART card. The main routines that would be included in the card ROM are the card interface routines and other housekeeping functions.

The information in the EPROM generally has to be erased with ultra violet light. This would imply that once the card has been programmed, the information cannot be erased in the card. Perhaps as a result the number of times that a series 05 (and before) Sky card could be killed and reactivated was limited. However the EEPROM versions are perhaps not limited in this respect. The EEPROM is more usable in SMART cards for one specific reason - it can be reprogrammed in the card. Of course it is now extremely dangerous to try and reprogram a card's EEPROM over the air. If the card has been hacked then the hackers would be able to watch the new data arriving and create a fix.

The actual card type used by Sky is a Motorola 6805 type card chip. It is not known at this stage what the version used by D2-MAC EuroCrypt is but it is believed to be similar. However the Sky version is EEPROM whereas most of the cards used on TV3, TV1000 and FilmNet are EPROM.

From this information, a memory map of a VideoCrypt SMART card can be guessed. The ROM area of the memory is the area where the main operational program and decryption algorithms are stored. The EEPROM area contains the service data, the pay per view data, the card identity data and the billing period data. The RAM is used for temporary storage of data.

The EEPROM contains the enabling data for each channel that the card user has paid for. The data entry for each channel would consist of a channel identifier, a billing period, a regional identifier, key data and authorisation data for the channel.

The design of a SMART card is complex and prototyping can take a few months. The ROM in the card has to be mask programmed. This essentially means that the programs to be stored in the ROM are designed as part of the chip. The procedure is straightforward.

The programs to be included in the ROM are developed on a SMART card emulator. This is a microprocessor development system that is configured to imitate a SMART card. It is hooked to a personal computer. The program developer will write the programs on the computer, test them, and if they run successfully, load them into the SMART card emulator. The SMART card emulator will then be plugged into a decoder to ensure that the programs work.

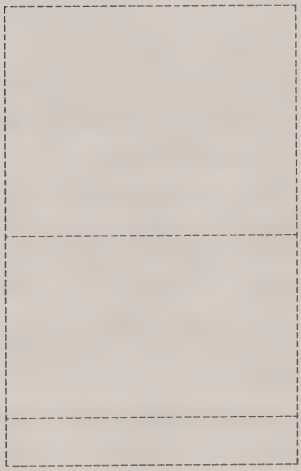
The programs will then be supplied on floppy disc to the chip manufacturer. The manufacturer will program an EPROM with the programs and send it to the card issuer for verification. Once the EPROM is checked, the manufacturer will then produce the chips in sample quantity. These chips will also be tested for correct operation. The chips can then be mass produced.

The chips are glued to a printed circuit board substrate with epoxy resin. The connection pins on the chip are wired to the connections on the substrate. The substrate connections are then wired to the connector array. The actual plastic card is injection moulded with an indent for the chip. The chip is then glued into the indent. The card is then tested to ensure that it is operational.

The SMART card at this stage will only have the bare minimum of data. There will be no service data in the EEPROM. This data is programmed into the card by the card issuer. In VideoCrypt's case, the personalisation stage would be carried out at News Datacom's Maidenhead facility.

Perhaps the most important aspect of this operation is testing. The programs in the smart card must undergo extensive testing before they are released on to the market. This test stage is essential as a problem that would require a new card issue may occur when the card is in the market.

A Smart Card Memory Map



MASKED ROM

This section contains the card's housekeeper programs and the Primary Decryption algorithm. This algorithm is used on all services.

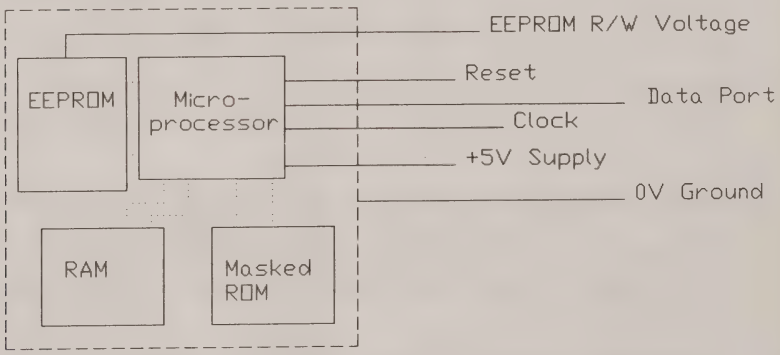
EEPROM

This section contains the service data, the authorisation, the card identity, the subsciber identity, the billing data and the period data.

RAM

This section is used by the decryption algorithm and other programs as a temporary storage area.

The Smart Card's Chip Structure



The Smart Card's microcontroller is fabricated on one chip. This chip contains EEPROM. If any attempt is made to scan the chip with an electron microscope, the EEPROM will be wiped. Since the design is all on a single chip the data flow between the memory areas cannot be directly examined.

SMART Card Operation

The SMART card is essentially a partial computer on a card. It is a partial computer because it requires other circuitry and inputs to operate. The first requirement is supply voltage. This is generally a 5 Volt DC supply.

The second requirement is a clock signal. This is a stable frequency square wave of 5 volts amplitude. This frequency is derived from a crystal in the decoder. The frequency used in the VideoCrypt card is 3.57 MHz.

The third requirement is a reset line. This is used to initiate the programs and routines in the card when the card is inserted into the socket.

The fourth optional requirement is the EPROM voltage. The EPROM programming voltage is high, typically over twenty volts. This voltage is only on for a few milliseconds every three seconds. The chip would generate too much heat if it was continually fed with high voltage. The EEPROM versions do not require the 21 Volts programming voltage. The programming voltage required by the card is signalled in the "Answer To Reset" block of data transmitted by the card.

The fifth requirement is the data port. The data flows to and from the card on one line. It is serial data. This port would be connected to the RAM in the card. The serial data would be clocked into the RAM. The microprocessor on the chip would then read the data in a parallel format. The data flows at 9600 Baud or at 9600 bits per second.

When the card is inserted into the decoder, the reset pin is activated. This zeroes the RAM and causes the microprocessor to select the boot-up program. This next routine in the program will verify that the card is valid for the period.

The card will then read the data from the decoder. This data, along with service data from the EEPROM, will be used in the decryption algorithm stored in the ROM. The product of the decryption algorithm will then be passed back to the decoder.

In the VideoCrypt system the information flowing to and from the smart card is useful in that it contains the addresses for cards being authorised and deauthorised as well as the actual decryption key. Other systems such as D2-MAC have a more complex packet structure.

This data is passed via the 8052 Housekeeper microcontroller to a secure microprocessor, the ZC404044 or ZC404047, where it is then used in a further algorithm to generate the seed for cutpoint generator at the start of every field or frame. The secure microprocessor is actually a Mask ROM version of the 6805 microcontroller. Of course this chip has been popped and the program is more or less common knowledge among European hackers.

Pay Per View is extremely easy to implement with a SMART card. The card user will purchase a number of credits or tokens each billing period. A typical number would be 99 tokens. The SMART card would be programmed so that the token counter would read 99 tokens. When ever the user wanted to watch a PPV film or event, a message would be shown on screen stating the number of tokens that the event is valued at. To watch the programme, the user would press the authorise or pay button on the front of the decoder. The decoder would then decrease the token register by the correct amount.

Each service could have a token register. The actual operation of the counting mechanism would be more complex. It would be too easy to intercept the token count value and substitute a continual 99 tokens. This type of hack is commonly used in computer games and is known as an "Infinite Lives POKE". At present the actual PPV algorithm for VideoCrypt lies mainly in the 8052. With the 09 card there are plans to introduce PPV. The subscriber will, according to some sources, have to pre-book the events.

SMART Card Security And Addressing

The VideoCrypt cards are valid once they leave the subscription centre. This means that they can be used in any VideoCrypt decoder. They can be deactivated over the air by Sky. The Quickstart cards are not valid until they have been activated by Sky.

When the kill occurs, a section of the EEPROM in the card is overwritten so that when the card is inserted into the decoder, it will not work. In order to reactivate the card, the program providers Sky send out a message to the decoder to reprogram the overwritten section of EEPROM.

This weakness was actually used to hack the VideoCrypt system though it was quickly discovered and countered. Of course this hack has reappeared for use with Quickstart cards.

Other systems using SMART card use over the air enabling. In this case, the cards cannot be used immediately. They have to be inserted into the decoder and the subscription centre has to be informed. The subscription centre will then activate the card. This method of addressing is more time consuming and thus less economical. It is basically a trade off between medium security and better security.

It appears that all of the VideoCrypt cards are shipped with the codes for all of the channels. During personalisation, the subscriber's channel allocations are entered into EEPROM. Therefore the subscriber will only be able to access the channels for which they have paid. Other channels will appear as being blocked.

The VideoCrypt is based on the Exclusion Principle. All of the smart cards on the system are active until they receive a kill signal. It is definitely not the most secure format as it is possible to get a card and keep it out of the decoder for a few months. As the kill signal is only transmitted aperiodically, the chances of the card being killed are reduced.

Of course the fact that the 09 and 07 VideoCrypt card issues have been hacked has destroyed VideoCrypt at least for this card issue. While the present 09 hack may have been knocked out by the ECM in June but the card addressing system is vulnerable.

Since the card addressing system can be cracked, it is therefore possible to reactivate the dead cards. Indeed given the procedure of the channel activation on the cards it is possible to activate each channel on a card.

The program for the hacker activation of cards and channels is known to exist. According to some sources it has been in operation since last year and a newer version works on the 09 card. The program's name is Phoenix and the cards are referred to as Lazarus cards.

Of course these Lazarus cards could be killed again. But the hackers already have a solution - the Sunblocker. The Sunblocker stops the kill signal from getting to the card by reading the card identity number and stopping any packets with that card's number from reaching it. The Sun reference is to Kelvin MacKenzie who is the head of BSkyB and who used to be the editor of the UK tabloid "The Sun". Other names such as the S#%tblocker have been mentioned.

Memory Cards

The vast majority of telephone cards are straight memory cards. To put it simply they are 265 bit serial eproms. The newer versions currently being tested are EEPROM.

One of the first companies to introduce the phone cards was France Telecom. Like most pioneers, it ended up with arrows in its corporate back. They were, in some senses, victims of their own success.

Whereas before phreaking was difficult and sometimes risky, the advent of the telephone cards made things anonymous and a lot easier. At first it was simply a case of some tape.

In terms of security, the telephone cards are abysmal. Since they are serial EPROMs, a number of hacks are possible. One of the earliest was the Infinite Lives hack. Since the EPROM required 21 to 23 Volts for a successful write operation, the write voltage was stopped from getting to the write pad on the smart card. A number of materials were used ranging from insulating tape to nail varnish.

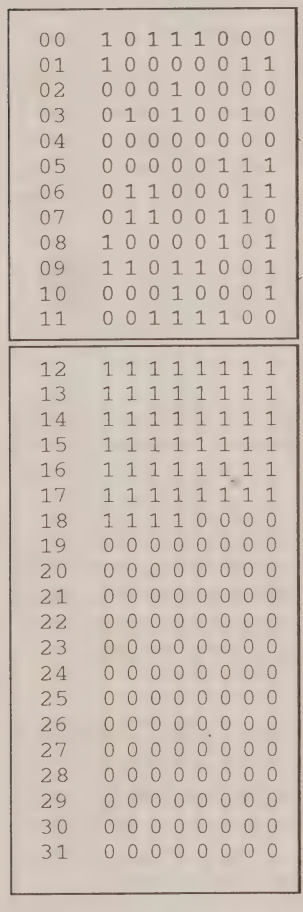
The 256 bits on the EPROM are arranged in 4 bit wide areas. The first 96 bits are the manufacturer and issuer codes. The other 160 bits are used to indicate the card value and the number of available credits. It is not possible to reprogram these cards to give higher values.

Other countries followed suit. Ireland introduced these EPROM phonecards and now in some areas, the card phones outnumber the conventional pay phones.

Given that the technology of the EPROM memory cards used for pay phones has been compromised for almost ten years, the people in Telecom Eireann who selected this technology were either very naieve or were taking one hell of a risk. Perhaps they were just typical bureaucrats who didn't have a clue about what can and cannot be hacked. What irritates me is that I have to pay telephone bills that pay for these people's mistakes. There are a number of designs for phonecard emulators that allow the user to make free phone calls.

Example Of Phonecard Memory Map

Bits 00 to 95 are the manufacturer/issuer area. This area is fuse protected and cannot be overwritten.



Bits 96 to 255 make up the programmable area of the card. These bits are set when the phone deducts a credit from the card. As this area is EPROM, these bits cannot be reset without wiping everything. The actual time and effort involved in taking the wafer out of the card and removing the epoxy resin is not worth it.

It is possible to read these memory cards as serial EPROMs. Radio Plans published a number of good articles on the subject a few years ago.

The PPV version of a memory card may not be that different from the model above. The manufacturer area of the card may well hold the key tables for the programmes. The Credits area may also hold a set of key tables for the relevant programmes. Of course as the decoder uses the key tables for each programme, then that particular table would be overwritten. It is unlikely that the memory cards would be used on their own for PPV applications. Even the VideoCrypt patent application mentions how insecure they are.

The ISO-7816 Protocol

The smart cards used on scrambling systems use a serial data link running at 9600 baud. All of the data is transferred via this link. The ISO-7816 part 3 specification covers the card transmission protocols.

When the card is inserted into the decoder, it is reset and it sends a packet of information to the decoder. This packet of information is known as the "Answer To Reset". This perhaps the most important packet sent by the card as it tells the decoder what kind of communications protocol is to be used and also what signals and voltages are necessary for operation.

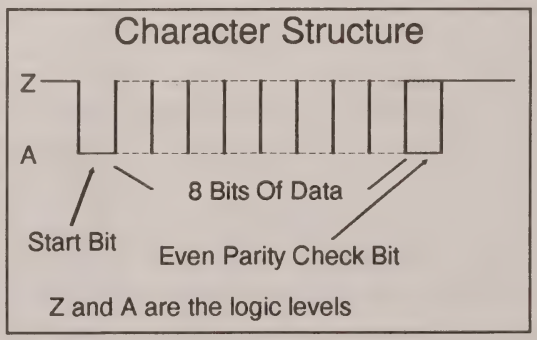
The structure of this ATR packet is shown in the diagram. Most of the smart cards in operation in Europe use the T=0 protocol. The T=1 version is a block transmission protocol whereas the T=0 protocol is a character transmission protocol.

The T=0 protocol is asynchronous, half duplex, active low reset and uses inverse convention. The term asynchronous means that the protocol is serial as opposed to parallel. With parallel transmission, some form of clocking signal has to be sent, in an asynchronous protocol, there is no separate clocking signal. Half duplex means that it is a talk - listen protocol. At any one time the data is flowing in only one direction. The inverse convention means that the data has to be inverted and the order of the bits has to be reversed to read it with an RS232 interface. The format is roughly equivalent to 8 data bits, 1 parity bit and 2 stop bits on the RS232 interface.

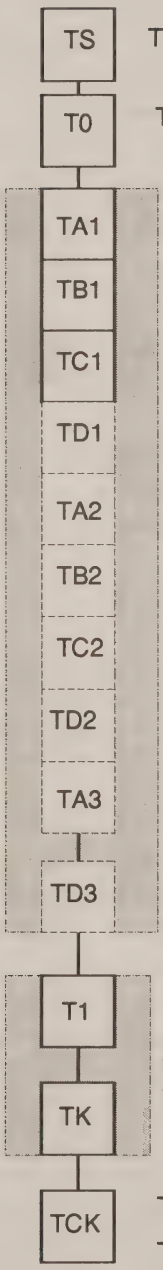
The T=0 protocol is a character based protocol. Each character is composed of ten bits. The first bit is a stop bit. The next eight bits are the data (a byte) and the last bit is the Even Parity check bit. This bit is used for error correction and always ensures that there is an even number of ones in the character.

The character structure is shown in the diagram opposite. The levels Z and A are the logic levels.

In the inverse convention (3Fh), the standard logic polarity



The Answer To Reset Packet Structure



TS — The Initial Character

T0 — The Format Character

The Interface Characters

TA1 — Clock Frequency

TB1 — Maximum Programming Current and Voltage

TC1 — Additional Guard Time Or Stop Bits Requested

TD1 — Subsequent Interface Characters And Protocol

If the TD_1 character is not transmitted in a packet then the protocol is assumed to be T=0 and no further interface characters follow.

This is exactly the situation with the official Sky (VideoCrypt) cards. They do not transmit a TD_1 character but the pirate VideoCrypt cards do transmit the TD_1 character.

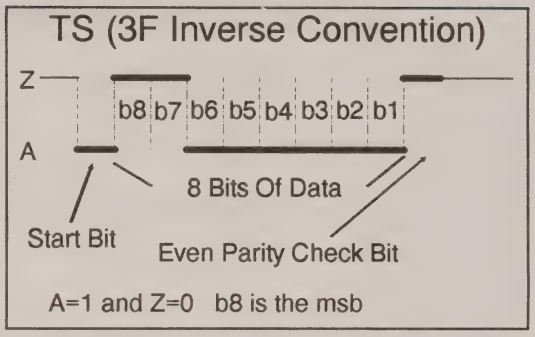
The Historical Characters (15 max)

These characters are card specific. They describe the type of card, the software issue, the ROM mask, the manufacturer code, the issuer code and the period for which the card is valid.

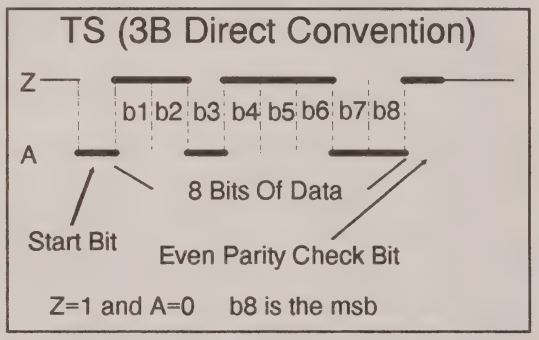
TCK — The Check Character

This character is not transmitted in T=0 only.

is reversed. (Z=0 and A=1). The order of the bits in the data is also reversed with the most significant bit being transmitted first.



In the direct convention (3Bh), the standard logic polarity is used, (Z=1 and A=0). The order of bits is normal with the least significant bit being transmitted first.



The error correction mechanism in the T=0 protocol is simple. If the parity check fails then a retransmission of that bit is requested by sending an A level in the guardtime after the parity bit. This causes a retransmission of the character. This form of error correction has no direct equivalent in the RS232.

The TS Character

This is the initial character of the ATR. It is either 3Fh or 3Bh. The 3Fh means that the inverse convention is used. The 3Bh means that the direct convention is used.

The T0 Character

This is the format character. This character specifies what interface characters and how many historical characters are transmitted. The breakdown on this character is shown in the inset box. The high nybble determines which interface characters are sent. The low nybble determines how many historical characters are sent.

The Interface Characters

The TA_1 Character

This character controls the clock selection. The VideoCrypt decoder is designed to handle two clock frequencies; 3.512 and 7.1424 MHz. The value for a 3.5712 MHz clock is 11h and for a 7.1424 MHz clock the value is 31h. The strange clock frequency has to do with the fact that the 9600 baud rate is derived from dividing 3.5712 MHz by 372.

The TB_1 Character

This character specifies the programming voltage and current required by the card. The most significant bit of this character is always zero. The next two most significant bits specify the maximum programming current factor in the case of the VideoCrypt ATR the most significant bits are 10b and this equates to a factor of 100. The bits b5 to b1 specify the programming voltage in volts. Again in the case of the VideoCrypt ATR (0101b) the programming voltage is 5 Volts.

The TC_1 Character

This character specifies how much extra guard time or stop bits to put between each character. In the VideoCrypt example, five stop bits are requested. The main idea here is to allow the card enough time to process each character before the next one arrives.

The TD_1 Character

In many respects this character is similar to the Format Character. The high nybble determines the presence of subsequent interface characters. The low nybble specifies the protocol to be used.

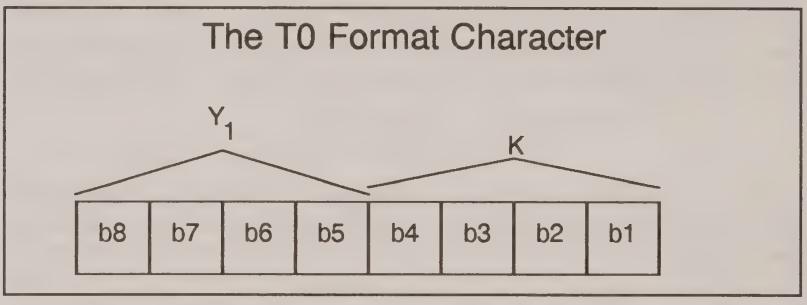
If the TD1 character is not transmitted, as indeed it is not in the official Sky cards, then the protocol is assumed to be T=0.

The T1 - TK Characters

These are the historical characters. They provide information about the card itself. The information in this area generally relates to the version of the software, the processor type, the card issuer, the card manufacturer and the date of manufacture.

The TCK Character

This is a final check character. It is the value necessary to ensure that the EXOR sum of all of the characters from T0 to TCK is zero. This check character is not transmitted if only the T=0 protocol is in operation.



Y1 indicates that there are interface characters to follow. The bitset indicates which characters they are.

b8=1 - TA1 (Clock Frequency)

b7=1 - TB1 (Maximum Programming Current and Voltage)

b6=1 - TC1 (Additional Guardtime or Stop Bits Requested)

b5=1 - TD1 (Subsequent Interface Characters and Protocol)

The K value indicates the number of historical characters transmitted. This is a numnber from 0 to 15 (0h to Fh).

On the following page there are examples of the answers to reset from three different cards. The first two are Sky cards and the last one is a pirate card. There are a number of characters that identify the Sky cards as being actual Sky cards. There are also some indicators that the actual card issue number and the month of issue are also included.

The actual function of some of the characters is not known - yet. It does however appear that there is a manufacturer's identifier and batch number in addition to an microprocessor identifier.

Sky Card Issue 07	Sky Card Issue 09	Pirate Issue 07
3F	3F	3F
7E	7E	FA
11	11	11
25	25	25
05	05	05
--	--	00
24	21	01
B0	B0	B0
05	12	02
00	00	3B
00	00	34
4D	4D	4D
59	59	59
00	00	00
01	00	81
80	00	80
53	53	
4B	4B	
07	09	
13	00	

The Sky cards do not send a TD1 character but the pirate card does.

The most important historical characters are the 4D 59 ones. The VideoCrypt decoder checks each card inserted to see if these bytes are present in the historical characters area at that particular position. If these characters are not found in these positions , the card is rejected. These appear to be the VideoCrypt identifiers. Perhaps they are partial initials of the designers.

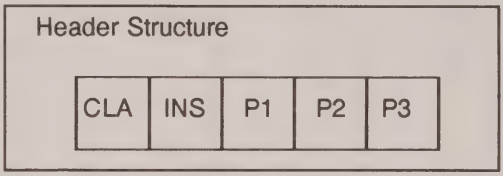
The B0 byte is not apparently essential though it does appear in all cards. This could be the microcontroller identifier that identifies the smart card (official) as a 6805 type.

The 53 4B characters may well be the identifiers for Motorola as in ASCII they are SK. Of course it is not clear what other characters identify the actual ROM Mask issue or indeed the program. Perhaps the characters before the VideoCrypt identifier are those to do with News Datacom's internal program identification.

The most obvious, if not a coincidence, are the two last characters of the official Sky cards. They identify the card issue as being 07 and 09 respectively. The last character may be an integer value as the 09 was a continuing subscription card. The subscription was taken in August 1993.

In the T=0 protocol, the decoder can send commands to the card. These commands are followed by a data transmission to or from the card. As the protocol is a character based protocol the card has some limited flow control capabilities. In addition to these capabilities the card can have the decoder turn on or off the programming voltage. This is achieved by using the Procedure Byte.

The decoder will send a five byte header to the card to initiate a command. The structure of the header is shown opposite.



The CLA is the class. For VideoCrypt this is always 53. INS is the instruction. This is the command instruction to be initiated. The P1 and P2 bytes are not used in VideoCrypt but are used in EuroCrypt. The P3 byte signals the length of the data.

Byte	Value	Meaning And Effect
	INS	Send (Do not turn on Vpp)
ACK	INS+1	Send (Turn on Vpp)
	NOT(INS)	Send Byte (Do not turn on Vpp)
	NOT(INS+1)	Send Byte (Turn on Vpp)
NULL	60h	Wait
SW1	SW1	End of transfer - wait for SW2 byte

After sending this header, the decoder then waits for the Procedure Byte. There is a number of types of procedure bytes. The main one is the Acknowledge or ACK byte. This tells the decoder how to proceed as regards transferring data and controlling the programming voltage.

The NULL byte signals that the decoder should wait for a new procedure byte. The status word bytes SW1 and SW2 transmit the card's status after the end of the command. The SW1 byte is used when there is a significant error. The SW1 error conditions are as follows.

6E Instruction class not supported

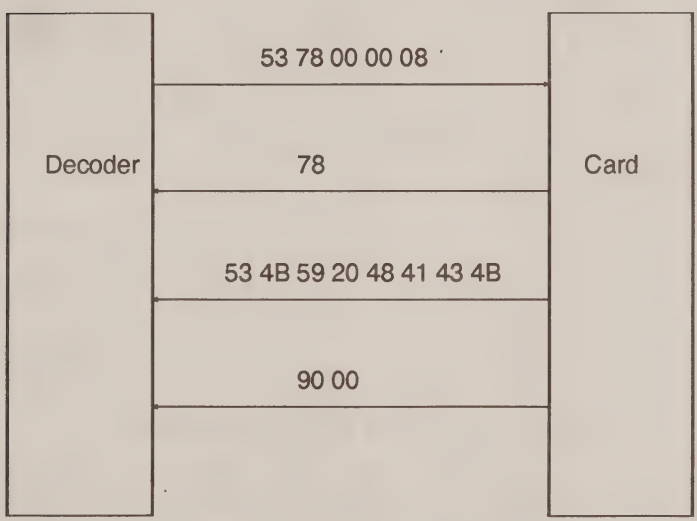
6D Unknown Instruction

6B Incorrect address or reference

67 Incorrect length

6F Unknown and its wrong anyway!

A normal command termination is represented by 90 00.

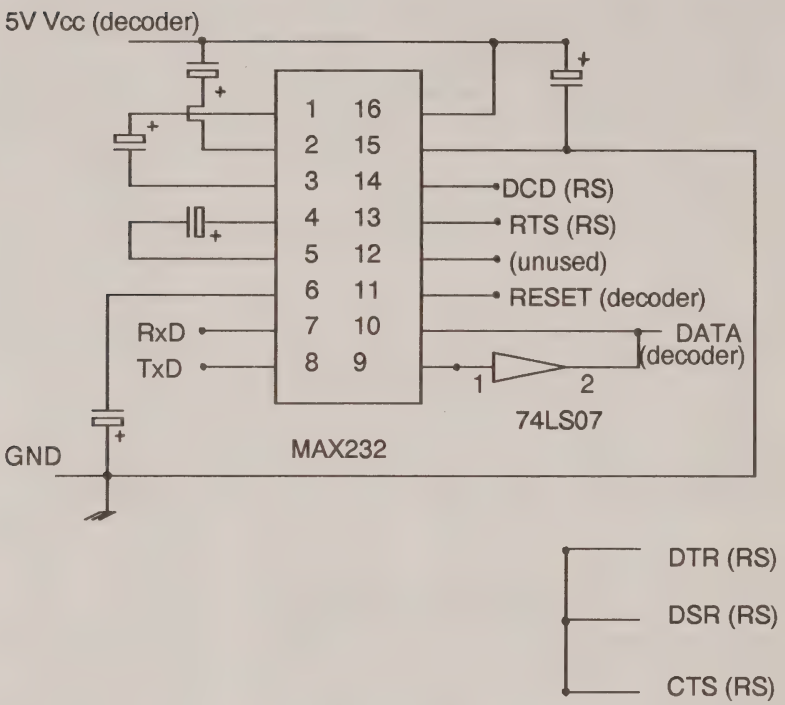


The diagram above is an example of the card - decoder traffic. The decoder sends the card a header requesting the eight byte decrypt key. The instruction for this command is 78h. The data is eight bytes long.

On many of the early card traffic monitoring programs this transaction would appear as the following.

53 78 00 00 08 78 53 4B 59 20 48 41 43 4B 90 00

A basic communications program would show up a similar block structure but a translation table would have to be entered to produce the proper results.



The Omigod & DDT Interface

This circuit is based on two chips. The MAX232 and the 74LS07. The MAX232 converts the levels from TTL to RS232 and vice versa. The 74LS07 is an open collector buffer. This allows a bidirectional operation of the data line to the decoder.

The capacitors are all 10uF 25V or greater. Electrolytic will do but for reliability Tantalum types are recommended.

This circuit can be built on Veroboard or on its own dedicated PCB. There are a number of PCB designs available for download on Special Projects BBS.

PCB Layout For Ho Lee Fook Hack Using PIC16C84

Note: The scale is approximately 1:1

Recommended Reading

The following list of magazines is by no means conclusive. They represent some of the best published information sources available.

Hack Watch News

The only source for information on scrambling systems and hacking. It is perhaps the best newsletter / magazine on signal security. All hacks that occur on any system are covered here.

(Subscription forms at back of book.)

Elektor Electronics

The best magazine for well designed projects. The level of complexity can range from amateur to professional. This is essential reading as it is the most technically interesting and advanced magazine on the market.

Subscription: UK £25, Ireland and Europe £32.

Elektor Electronics,
World Wide Subscription Service Ltd.,
Unit 4, Gibbs Reed Farm,
Pashley Road, Ticehurst,
East Sussex, TN5-7HE, UK.

Eletronique Radio Plans

This is the most famous magazine in Europe. It published the original hack on the Discret system. It also publishes articles of the highest quality. Even if you cannot read French, this magazine is essential for the sheer quality of the technical material.

Subscription: France 288F, Europe 364F

Electronique Radio Plans,
2 a 12, Rue de Bellevue - 75940
Paris Cedex 19, France.

Recommended Reading

Interspace

The only weekly newsletter on the industry. Covers all aspects from regulatory to technical. It is the oldest and most respected newsletter in Europe.

Subscription: UK £299, Europe £399, Rest Of World £359

European Satellite & Space News,
Subscriptions Dept., The Counting House,
21 Market Street , Alton,
Hampshire, GU34-1HA, UK.

Transponder

Transponder is a well produced newsletter aimed specifically at those of use who like to flit from satellite to satellite. The newsletter is published twice monthly and is therefore more up to date than the monthly magazines.

There are no irrelevant adverts or features. The contributors to the newsletter are knowledgeable on the subject and in many cases have been in the business since the early eighties. It is edited by David Thorpe.

Subscription: UK £60.00 Europe £70.00 £85.00

TRANSPONDER,
PO Box 112, Crewe,
Cheshire, CW2 7DS, UK

Telephone: +44 270 580099

McCormac's
Hack Watch News

Annual Subscription Details:

Europe: IR£49.95 Rest Of World: IR£77.00

Corporate Subscription: IR£220.00

Terms: Access, MasterCard, Visa or Bank Draft.

☆ A subscription to Hack Watch News also gives you access to the Special Projects BBS.

☆ Subscribers also can purchase books listed in the Recommended Reading section at a discounted price.

Send To: Hack Watch News, MC2, 22 Viewmount, Waterford, Ireland.

Or Fax To: +353-51-73640

Card Type: .....

Card Number: .....

Card Expiry: .....

Name On Card: .....

Subscription Total: .....

Name: .....

Address: .....

Address: .....

Address: .....

Country: .....

Telephone: .....

McCormac's
Hack Watch News

Want to find out about the EuroCrypt Omigod hack?

Will there be an 09 Sky hack that will last?

How does Phoenix work and what will it do to VC?

You might will find the answers in Hack Watch News.

If a system is hacked then the details will appear in Hack Watch News.

How will you really know what is happening if you don't read it?

☆ Send Two Pounds (IR) for a sample issue

Hack Watch News, (SI)

MC2 (Publications Division), 22 Viewmount, Waterford, Ireland.

Orders only accepted on Original Black Book Form

Name:.....

Address:.....

Address:.....

Address:.....

Country:.....

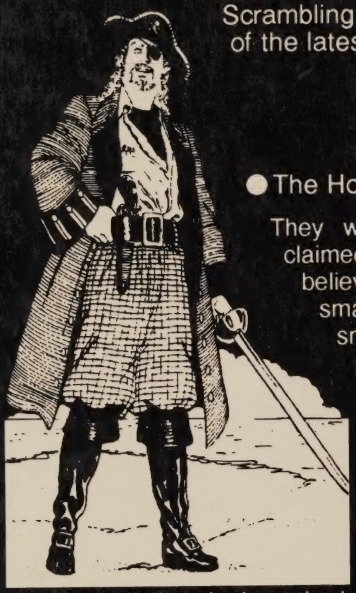
Telephone:.....

Warning

This page may have to be removed under conditions for distribution in certain countries.

```
const unsigned char adult_keys[96] = {
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x56, 0xf2, 0xb6, 0x4f, 0xc9, 0xbd, 0x2a, 0xb3,
0x9d, 0x81, 0x5d, 0xe0, 0x05, 0xb5, 0xb9, 0x26,
0x67, 0x3c, 0x65, 0xa0, 0xba, 0x39, 0xc7, 0xaf,
0x33, 0x24, 0x47, 0xa6, 0x20, 0x1e, 0x14, 0x6f,
0x48, 0x9b, 0x4d, 0xa6, 0xf9, 0xd9, 0xdf, 0x6e,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00
};
if (msg[1] > 0x4a) key = adult_keys + 48;
else if (msg[1] > 0x43) key = adult_keys + 40;
else if (msg[1] > 0x3a) key = adult_keys + 32;
else if (msg[1] > 0x33) key = adult_keys + 8;
else key = adult_keys;
```

European Scrambling Systems is the "bible" of the black arts of signal security. Now in European Scrambling Systems 4, John McCormac analyses all of the latest hacks and scrambling systems.



In This Version...

- The Ho Lee Fook and OMIGOD Hacks

They were hacks that Sky and News Datacom claimed were impossible. The hackers did not believe them. The Ho Lee Fook was a hacker smart card that completely replaced the official smart card. The OMIGOD hack is a computer program that allows the computer to control the decoder. For over a year VideoCrypt was totally hacked. Read how the hacker algorithms work - with actual C source code and diagrams.

- The Next VideoCrypt Hack - DDT

While Sky have issued a 09 card and temporarily knocked out the hacker cards, the latest hack removes the need for the presence of a Sky card. It also destroys the Pay Per View capability of VideoCrypt. It uses the same type of interface as the OMIGOD hack and may well leave VideoCrypt open to an American style attack.

- EuroCrypt Cracked

Like VideoCrypt, EuroCrypt-M has been hacked since 1992. This system used conventional algorithms. The result has been a disaster. Even in the event of ECMs, the keys are quickly obtained. Read how this system is the next candidate for an OMIGOD hack.

Warning

The information contained in this book is for educational use only. The publishers and the author do not assume any liability for the use or misuse of the information herein. In certain countries the use of certain circuits and techniques may be prohibited by law.

Waterford University Press,
MC2 (Publications Division),
22 Viewmount, Waterford Ireland.

Voice & Fax: +353-51-73640
BBS: +353-51-50143 V32bis V.Fast
email: mc2@cix.compulink.co.uk

ISBN:1-873556-03-9 **IR£30.00**

This book must not be sold in Ireland at a price greater than IR£30.00.

Recommended UK Retail Price: UK£32.00